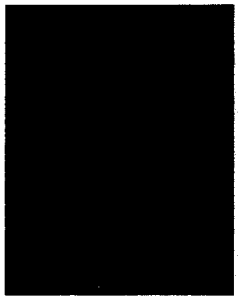


Professor Edward B. Burger is Professor of Mathematics in the Department of Mathematics and Statistics at Williams College. He received his Ph.D. from The University of Texas at Austin. Professor Burger is the author of more than 30 scholarly papers and 12 books on mathematics. In 2006 he was listed in the *Reader's Digest* annual "100 Best of America" special issue as "Best Math Teacher"; in 2007 Williams College awarded him the Nelson Bushnell Prize for Scholarship and Teaching.

"The Teaching Company has become a serious force in American education."

— ***The Wall Street Journal***

"One could devote a lifetime to lectures from the Teaching Company and it would be a life well spent."

-- ***AudioFile*® magazine**

"I've never made a secret of the fact that I consider the products from The Teaching Company to be the best value in college-level education today."

— **Harold McFarland, Regional Editor**
Midwest Book Review

THE TEACHING COMPANY®
4151 Lafayette Center Drive, Suite 100
Chantilly, VA 20151-1232
Phone: 1-800-TEACH-12 (1-800-832-2412)
Fax: 703-378-3819
www.TEACH12.com

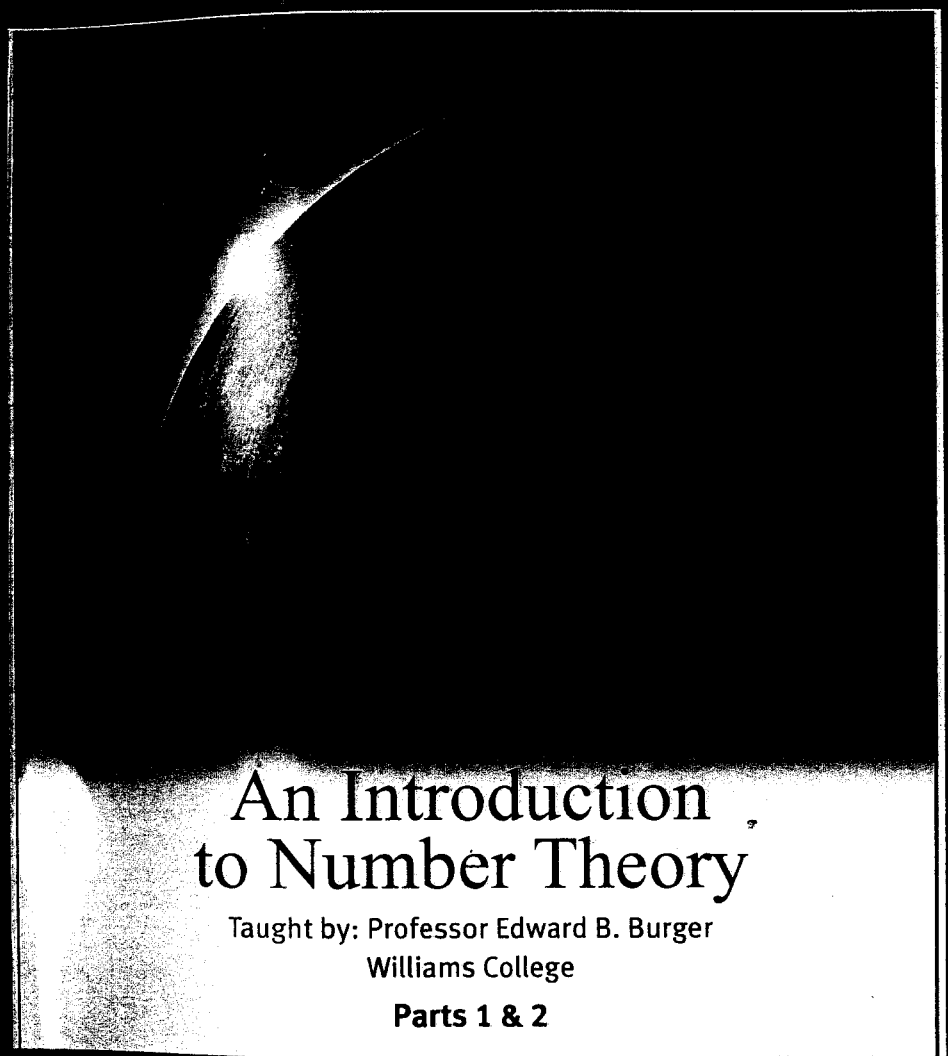
An Introduction to Number Theory, Parts 1 & 2

1495

Cover image: Earth Eclipsing the Sun. © Digital Art/CORBIS.

THE GREAT COURSES

Science & Mathematics



An Introduction to Number Theory

Taught by: Professor Edward B. Burger
Williams College

Parts 1 & 2

Course Guidebook

THE TEACHING COMPANY

An Introduction to Number Theory

Parts I & II

Edward B. Burger, Ph.D.

PUBLISHED BY:

THE TEACHING COMPANY
4151 Lafayette Center Drive, Suite 100
Chantilly, Virginia 20151-1232
1-800-TEACH-12
Fax—703-378-3819
www.teach12.com

Printed in the United States of America

Edward B. Burger, Ph.D.

Professor of Mathematics
Department of Mathematics and Statistics, Williams College

Edward B. Burger is Professor of Mathematics in the Department of Mathematics and Statistics at Williams College. He graduated summa cum laude from Connecticut College in 1985, earning a B.A. with distinction in Mathematics. In 1990 he received his Ph.D. in Mathematics from The University of Texas at Austin and joined the faculty at Williams College. For the academic year 1990–1991, he was a postdoctoral fellow at the University of Waterloo in Canada. During three of his sabbaticals, he was the Stanislaw M. Ulam Visiting Professor of Mathematics at the University of Colorado at Boulder.

Professor Burger's teaching and scholarly works have been recognized with numerous prizes and awards. In 1987 he received the Le Fevere Teaching Award at The University of Texas at Austin. Professor Burger received the 2000 Northeastern Section of the Mathematical Association of America Award for Distinguished College or University Teaching of Mathematics and the 2001 Mathematical Association of America's Deborah and Franklin Tepper Haimo National Award for Distinguished College or University Teaching of Mathematics. In 2003 he received the Residence Life Academic Teaching Award at the University of Colorado. Professor Burger was named the 2001–2003 George Polya Lecturer by the Mathematical Association of America and in 2004 was awarded the Chauvenet Prize—the oldest and most prestigious prize awarded by the Mathematical Association of America. In 2006 the Mathematical Association of America presented him with the Lester R. Ford Prize, and he was listed in the *Reader's Digest* annual "100 Best of America" special issue as "Best Math Teacher." In 2007 Williams College awarded Professor Burger the Nelson Bushnell Prize for Scholarship and Teaching; that same year, he received the Distinguished Achievement Award for Educational Video Technology from The Association of Educational Publishers. Professor Burger's research interests are in number theory, and he is the author of 12 books and more than 30 papers published in scholarly journals. He coauthored with Michael Starbird *The Heart of Mathematics: An invitation to effective thinking*, which won a 2001 Robert W. Hamilton Book Award. They also coauthored a general audience trade book titled *Coincidences, Chaos, and All That Math Jazz*.

This is Professor Burger's third course for The Teaching Company. He previously taught *Zero to Infinity: A History of Numbers*, and he also co-taught *The Joy of Thinking: The Beauty and Power of Classical Mathematical Ideas*.

In addition, he has written seven virtual video textbooks on CD-ROM with Thinkwell and has starred in a series of nearly 2,000 videos that accompany the middle school and high school mathematics programs published by Holt, Rinehart and Winston.

Professor Burger has served as chair of various national program committees for the Mathematical Association of America; he serves as associate editor of the *American Mathematical Monthly*, and he is a member of the board of trustees of The Educational Advancement Foundation.

Professor Burger is a renowned speaker and has given more than 400 lectures around the world. His lectures include keynote addresses at international mathematical conferences in Canada, France, Hungary, Japan, and the United States; mathematical colloquia and seminars at colleges and universities; presentations at primary and secondary schools; entertaining performances for general audiences; and television and radio appearances including WABC-TV, the Discovery Channel, and National Public Radio.

Acknowledgments

Lucinda Robb had been encouraging me to return to The Teaching Company classroom for nearly two years. I want to sincerely thank her for her cheerful patience and constant enthusiasm. If it were not for her encouragement and support, I would not have had the wonderful opportunity to create this course and its historical counterpart, *Zero to Infinity: A History of Numbers*.

I also wish to express my sincere appreciation to the *Introduction to Number Theory* team at The Teaching Company, who made the entire process—from preproduction through postproduction—so pleasurable. Marcy McDonald provided excellent editorial suggestions and comments about the course structure. Zach "Zax" Rhoades was an outstanding producer who beautifully integrated the lectures with the visual elements. Tom Dooley and Jim Allen were the technical masterminds performing magic in the control room.

Within the world of mathematics, I wish to express my deepest gratitude to Professor Deborah J. Bergstrand from Swarthmore College. Professor Bergstrand provided invaluable and insightful suggestions that enhanced these lectures. Her contributions and dedication to this project were spectacular, and I thank her for all her efforts and for her friendship. From The University of Texas at Austin, I wish to thank my Ph.D. advisor, Professor Jeffrey D. Vaaler, who was the first to show me the beauty, wonder, and mystery hidden within the world of number theory.

Table of Contents
An Introduction to Number Theory

Table of Contents
An Introduction to Number Theory

An Introduction to Number Theory

Scope:

The study of numbers—an area of mathematics now known as *number theory*—dates back to antiquity. Through the intervening millennia, creative and curious people around the world have pondered the meaning and nuance of numbers. Today, number theory is one of the exciting and active branches of modern mathematics that have seen great breakthroughs, such as Fermat's Last Theorem; great applications, such as public key cryptography; and great open questions, such as the Riemann Hypothesis—a complete and correct proof of which would entitle its author to a million-dollar prize.

In this course we will begin at the beginning and delve into the basic structure of numbers. We will then move into the study of surprising and stimulating results that have both tickled and confounded humankind for thousands of years. Beyond the ticker tape of numbers that possess clear and elegant patterns, we will explore the enigmatic prime numbers, discover the synergy between rational and irrational numbers, visit the world of algebraic and transcendental numbers, and journey into several modern areas including elliptic curves—a critical key to unlocking the proof of Fermat's Last Theorem after 350 years. While some mathematical confidence on the part of the student would be useful, these lectures will always paint a big picture of the main ideas in an accessible and nontechnical fashion before highlighting the intriguing and delicate details.

Lecture One

Number Theory and Mathematical Research

Scope: In this opening lecture we will take our first steps into the abstract world of number theory and see how it fits within the larger mathematical landscape. We will come to view mathematics as a living and growing intellectual pursuit, and mathematicians both as artists creating new worlds and as explorers attempting to better understand our universe. Throughout their scholarly journey, mathematicians navigate through the subtle and narrow confines of truth. Mathematicians create *conjectures*—highbrow verbiage for educated guesses. Those conjectures are either proven to be true, in which case they are designated as *theorems*, or a counterexample is discovered demonstrating that the conjecture, in its generality, is false. If true, then the mathematical mind asks if the result can be extended or generalized. If false, then the mathematician wonders if the statement can be salvaged. Here we will describe this intellectual exploration and how it allows the frontiers of mathematical knowledge to move forward. Number theory is one of the oldest and most important branches of mathematics. At its very essence, number theory is the study of the natural numbers: 1, 2, 3, 4, and so forth. More precisely, it is an intellectual discipline concerned with the arithmetical structure of the natural numbers and the extensions and generalizations of such numbers. We will introduce some of the main branches of number theory, foreshadowing the journey ahead. After this overview of the number theoretic ideas we will discover throughout our course, we will close with a proof of our first mathematical truth: the whimsical "theorem" asserting that every natural number is interesting.

Outline

I. Welcome to the world of number.

A. The motivation for number theory.

1. We begin with the counting numbers, which we call the *natural numbers*: 1, 2, 3, 4, 5, … .

2. Numbers evolved from useful tools to objects of independent interest.

3. The true motivation behind the theory of numbers comes from a desire to study the simplest numbers: the natural numbers. One of the fundamental recurring themes throughout this course is that when we explore "simple" objects in great depth, we uncover otherwise invisible delicate structure.

B. Different types of numbers.

1. The natural numbers: 1, 2, 3, 4, 5, … .

2. The integers: … , −3, −2, −1, 0, 1, 2, 3, … .

3. The ratios of integers (fractions) are called *rational numbers*.

4. The numbers that are not ratios are called *irrational numbers* (numbers that are not rational).

5. The decimal numbers are called *real numbers*, which can be viewed as points on a number line.

C. The surprising synergy between numbers.

1. Once we identify different types of numbers, they take on a life of their own, dictated by the laws of nature and mathematics, and we can study their rich and intricate personalities.

2. We will see many surprising connections between these different numbers. This interplay and synergy between numbers will be another recurring theme throughout our course.

II. The culture of mathematics.

A. Mathematics is an ever-growing area of active research.

1. Mathematics is an abstract universe of both nature and the mind.

2. Mathematicians are at once explorers and artists.

3. Mathematics is a search for structure.

B. Moving the frontiers forward.

1. Most mathematics is not yet understood.

2. Mathematicians, as a community, build on each other's works to move the boundaries of our understanding outward.

3. We will begin with some basic self-evident truths—known as *axioms*—and build upward.

4. We will then study simple objects and search for patterns.

5. Patterns lead to conjectures, which in turn can lead to theorems.
6. New theorems are discovered, proofs are created, and then the mathematics community reviews and accepts the new results.

C. The power of proof.
1. Mathematics is built on the notion of rigorous proof.
2. Mathematicians are at once artists and lawyers.
3. Our course will celebrate the creative art of rigorous proof.

III. What is number theory?

A. Analytic number theory: a focus on primes.
1. The prime numbers are those natural numbers greater than 1 that cannot be written as a product of two smaller natural numbers.
2. The first few prime numbers are 2, 3, 5, 7, 11, 13, and 17.
3. The prime numbers form the building blocks for all natural numbers: Every natural number greater than 1 is a product of prime numbers.
4. Are there infinitely many prime numbers?
5. The prime number theorem, proved in 1896, in some sense reveals what proportion of natural numbers are primes: As we consider larger and larger values of n, the number of primes up to n approaches the quantity $n/(\log n)$. One of the most important open questions in mathematics asks if this result can be improved. The question is now known as the *Riemann Hypothesis*.
6. This area of number theory is known as *analytic number theory* because it employs the techniques of calculus to establish the truth of its results.

B. Algebraic number theory: a focus on arithmetic.
1. Suppose we have an equation that just involves addition, subtraction, and multiplication of natural numbers. Can we always find natural numbers that are solutions? Such equations are called *Diophantine equations*.
2. For example, if we consider the equation that arises from the Pythagorean Theorem: $x^2 + y^2 = z^2$, then we see that $x = 3$, $y = 4$, and $z = 5$ are natural numbers that give a solution. Are there others? Infinitely many?

3. As we will see, the famous "Fermat's Last Theorem" states that a related equation has no natural-number solutions. Finding a complete proof of this assertion remained one of the most prized open questions in mathematics for over 350 years until it was finally established in the mid-1990s.
4. The study of solutions to these types of equations will lead us to discover a generalized notion of integers and then a generalization of the prime numbers.
5. Because this area of number theory is inspired by a search for solutions to equations, it is known as *algebraic number theory*.
6. Given that both analytic and algebraic number theory involve the study of primes and their generalizations, it will not be surprising to see a synergistic interplay between these two branches of the theory of numbers.

IV. The vistas ahead in this lecture series.

A. Elementary number theory.
1. We start by discovering some interesting patterns involving natural numbers. These attractive patterns of numbers not only hold an independent aesthetic appeal, but they will also be extremely useful tools as we move to deeper areas of number theory.
2. These early explorations into pattern will also provide us with the opportunity to craft our own conjectures and to become accustomed to the world of rigorous proof.

B. Analytic number theory will formally introduce the prime numbers and study their central role in the universe of number.

C. Modular arithmetic.
1. Combining the properties of primes with the "clock arithmetic" of cycles, we will discover a world of arithmetic involving division that focuses on remainders rather than quotients.
2. As we will discover, this classical study holds one of the most important modern applications of number theory: public key cryptography.

D. Algebraic number theory. In our attempt to find solutions to certain equations, we will come upon parallel universes of number

that will lead us to rethink the basic mathematics we were taught in school.

E. Algebraic geometry.
1. Here we will combine the power of algebra and geometry to discover an important connection between solutions to certain equations and points on certain curves.
2. The interplay between number theory and geometry is one of the most profound elements of modern number theory.

F. Algebraic and transcendental numbers.
1. Here we will explore whether there are any other numbers beyond those that are the solutions to the equations we studied in algebraic number theory.
2. This question remained unanswered for thousands of years until the definitive answer was finally found in the mid-1800s, which in the scope of mathematical history was "yesterday."

G. Continued fractions.
1. Beyond writing numbers as familiar decimals, we will discover an alternative manner to express numbers that is much more sympathetic to number theory inquiries.
2. This manner of expanding numbers allows us to build insights into many phenomena, from why 22/7 is so close to π, all the way to why we have a 12-note chromatic musical scale.

H. Throughout the course, we will offer applications and stories both famous and whimsical that will not only enhance the number theory at hand but will provide a context within which we can better appreciate our discoveries about the structure within the world of number.

V. Every number is interesting.

A. A personal passion for number theory.
1. The intrigue of number—a notion that is at once basic and profound.
2. The creativity and originality involved in crafting a proof.
3. Painting an abstract portrait of beauty and detail.
4. Viewing mathematical proof as a new form of art.

B. "Theorem": Every natural number is interesting.
1. The "proof" of this whimsical assertion illustrates an argument known as *mathematical induction*.

2. We consider the first natural number, 1. It is the smallest natural number, and thus it is certainly interesting.
3. The next natural number, 2, is the smallest even number, which is interesting.
4. Could there be a natural number that is *not* interesting? If so, then there must be a smallest one; that is, the smallest natural number that is not interesting. In other words, every natural number less than this number *is* interesting, and this number is the first natural number that is *not* interesting—but isn't *that* interesting? This exclamation concludes our humorous proof.
5. The world of number theory is indeed interesting. Our journey ahead is teeming with deep ideas, profound insights, and incredible discoveries. While we will see serious mathematics revealed in details and proofs, we will always place those technical points in context within the panorama of number.

Questions to Consider:

1. Give several examples of situations in which logical proofs are required.
2. Returning to the whimsical mathematical proof that every natural number is interesting, suppose that all the numbers from 1 to 20 are previously known to be interesting. How can you use this fact to show that the number 21 *must* also be interesting?

Lecture Two

Natural Numbers and Their Personalities

Scope: The most natural place to begin our journey into number is with the numbers we have always counted on—the natural numbers: 1, 2, 3, 4, and so forth. In this lecture we celebrate the main characters of our story and foreshadow the methods by which we uncover and establish the truth of theorems. Of course, there are infinitely many natural numbers, and making that reality intuitive, even today, is much more challenging than it first appears. As we will discuss, most numbers, for example, cannot even be named. But can *all* numbers be understood in either practice or in theory? Here we will highlight the remarkable reality that mathematical thinking allows us to verify truths about *all* numbers—the unending collection of values, most of whom we will never name, imagine, or comprehend. This reality will underscore the power of rigorous proof. Once we introduce the main characters of this course, we can move to the means by which we will study their personalities; these traits arise through the introduction of arithmetic. It is this marriage of number and arithmetic that gives birth to notions of number theory. We will close this lecture with some basic but striking arithmetical observations—some, we will see, are provable theorems, while others remain hidden in a veil of mystery.

Outline

I. Speaking the language of numbers.
   - **A.** Natural numbers are the numbers in the collection $\{1, 2, 3, 4, \ldots\}$.
   - **B.** Integers consist of the natural numbers together with their negatives and zero.
   - **C.** Rational numbers are all ratios of integers. Specifically, a rational number is a number that can be expressed as a/b, in which a is an integer and b is a natural number.
   - **D.** Real numbers are all "decimal numbers," that is, the numbers that correspond to points on the number line.

II. Do large numbers have any intuitive meaning to us?
   - **A.** The endless stream of natural numbers.
     1. Clearly there are infinitely many natural numbers, and our goal in number theory is to attain a deep understanding about these objects.
     2. The desire to understand an infinite collection of objects in a finite amount of time is the fundamental feature that makes this inquiry both subtle and abstract—and thus generates much of its intrigue.
   - **B.** Naming the numbers.
     1. From a practical point of view, our understanding of numbers is dictated by their utility in our everyday lives.
     2. Some early cultures counted "1, 2, many." Today we are familiar with millions and trillions.
     3. As number theory enthusiasts, we wish to study all of the natural numbers, so naming them becomes an issue. Even silly names can be useful, such as "googol" and "googolplex," the origins of which are amusing stories.
     4. However, there are infinitely many numbers, and most of them—from the point of view of language—have not been named.
   - **C.** How large is our universe?
     1. Not all quantities within our universe can be named.
     2. The size of our universe is approximately 10^{79} atoms.
     3. Skewes number, $10^{10^{10^{34}}}$, is believed to be the largest number that appears in a significant mathematical theorem.
     4. While these numbers are so large that they might have no intuitive meaning to us, such sizes are insignificant from a number theory prospective because there are infinitely many numbers greater than these relatively tiny values.
     5. Here in this field of inquiry we wish to study those objects that we, in practice, will never see—numbers whose names we'll never utter.
   - **D.** The power of proof.
     1. We wish to make discoveries about endless lists of numbers—we make conjectures and strive to show that they are indeed valid.

2. We cannot simply check each natural number to verify a conjecture.
3. We rely on logical and abstract thinking and craft a rigorous proof.

III. The personality of numbers.

A. Searching for structure within the numbers.
1. We explore the numbers and search for interesting patterns.
2. Those patterns often lead to important insights into the structure of numbers.
3. We look at patterns within the numbers 1, 4, 9, 16, … .

B. The central notion of divisibility.
1. We look at even and odd numbers and the patterns they exhibit.
2. One important way of detecting the personality of a natural number is to factor it.
3. The factors are also known as *divisors*.
4. The notions of divisibility and divisors are the centerpieces of number theory.

C. Products of consecutive even or odd numbers (plus 1).
1. We examine a pattern within products of evens (plus 1).
2. We prove the pattern and discover a theorem.
3. We look at a similar pattern with odd numbers.

IV. Collatz's question.

A. Introducing the famous "$3n + 1$ question."
1. Given a natural number n, we use it to generate a list of numbers by the following process.
2. If n is even, then the next natural number on our list is $n/2$; if n is odd, then the next natural number on our list is $3n + 1$.
3. We now apply the same procedure with this new number to produce the next number on the list and continue.
4. This sequence was first studied by Lothar Collatz in 1937.

B. Illustrations and examples.
1. If we start with 1, we see: 1, 4, 2, 1, 4, 2, 1, … . Thus if we generate a 1, we know the rest of the list will just repeat: 1, 4, 2, 1, 4, 2, 1, and so forth.
2. If we start with 2, we see: 2, 1, 4, 2, 1, and so forth.

3. If we start with 3, we see: 3, 10, 5, 16, 8, 4, 2, 1, 4, 2, 1, and so forth.
4. If we start with 4, we see: 4, 2, 1, 4, 2, 1, and so forth.
5. If we start with 11, we see: 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1, 4, 2, 1, and so forth.

C. Searching for a pattern: the known.
1. It appears that no matter which we start with, the list always eventually becomes an endless run of 1, 4, 2, 1, 4, 2, 1, … .
2. If we start with the modest number 27, the process will produce a list of 111 numbers before we finally see our first 1. Within those first 111 numbers we would see numbers as large as 9,232. But we do finally settle down to the familiar 1, 4, 2, 1, and so forth.
3. Every natural number up to around 10^{18} has been used as the starting value. In each case, the list finally settles down to the repeating 1, 4, 2, 1, and so forth.

D. The endless unknown.
1. Collatz conjectured that starting with *any* natural number, the list will eventually settle down to 1, 4, 2, 1, and so forth.
2. This remains one of the most famous open questions in elementary number theory.

V. Discovering your power through number theory.

A. Powers of 2. Let's produce the first few powers of 2: $2^1 = 2$; $2^2 = 4$; $2^3 = 8$; $2^4 = 16$; $2^5 = 32$; $2^6 = 64$; … ; $2^9 = 512$; … ; $2^{24} = 16{,}777{,}216$.

B. A screed of digits.
1. What are the first (left-most) digits we see in the above numbers? 2, 4, 8, 1, 3, 6, and then later, 5.
2. Are there powers of 2 that begin with the missing two nonzero digits, 7 and 9?
3. One can check that $2^{46} = 70{,}368{,}744{,}177{,}664$ and $2^{53} = 9{,}007{,}199{,}254{,}740{,}992$.
4. Thus we see that every digit from 1 to 9 is the first (left-most) digit for some power of 2. Is there a power of 2 that begins with 10, or 11, or 12? Is there a power of 2 that begins with your social security number? How about your social security

number, followed by your birth date, followed by your cell phone number (including the area code)?

C. A surprising theorem.
   1. As amazing as it might at first seem, there is a theorem that asserts that given any natural number n, there exists a power of 2 whose left-most digits agree with the digits of the given natural number n.
   2. The truly amazing aspect of this assertion is that this result can be proved for all natural numbers.

D. The ideas involved in the proof of the theorem.
   1. At the very end of this course, we will have developed enough mathematical machinery to appreciate the ideas behind why this result is true.
   2. As we will discover, to prove this result, we must travel beyond the world of natural numbers and employ results involving the irrational numbers. This connection will be our final illustration of the incredible synergy between the many different types of numbers.

Questions to Consider:

1. Consider the numbers 61 and 64, which are clearly 3 apart. In what ways do their *arithmetic* personalities differ?
2. Verify that the "$3n + 1$ question" has an affirmative answer if you start with 7.

Lecture Three

Triangular Numbers and Their Progressions

Scope: On the one hand, studying Pythagoras, the celebrated ancient Greek lover of number from the 6th century B.C.E., is a natural beginning to this lecture. On the other hand, it seems fitting to open with the great 19th-century German mathematician Carl Friedrich Gauss, who has contributed either directly or indirectly to nearly every advance of every corner of number theory and is known as the "Prince of Mathematics." Here we will bridge both ages and cultures to study a common mathematical curiosity that each of these two prominent figures explored—the collection of figurate numbers known as *triangular numbers*. Triangular numbers can be defined intuitively as the number of billiard balls required to create larger and larger equilateral triangles. As we will see, this basic idea leads to some very profound theorems about the natural numbers. This discussion will foreshadow our later discussion on searching for natural-number solutions to certain equations—an area now known as *Diophantine analysis*. The triangular numbers have important implications within both our everyday world and the world of number theory. Generalizing these numbers will allow us to discover the central mathematical concept of arithmetic progressions. Arithmetic progressions are lists of numbers for which the difference between any two adjacent terms is always the same value. Both the even numbers (2, 4, 6, 8, and so forth) and the odd numbers (1, 3, 5, 7, and so forth) are examples of arithmetic progressions. These arithmetic progressions of numbers are central and useful objects within the study of numbers and will follow us throughout our studies.

Outline

I. The mathematical life and mind of Carl Friedrich Gauss.
   A. Gauss's early days.
      1. Carl Friedrich Gauss was born on April 30, 1777, in Germany. His father was a bricklayer and did not encourage his son to pursue advanced mathematics.

2. However, it was clear from a very early age that Gauss was a true mathematical child prodigy. There are many stories about young Gauss.
3. One famous story involves Gauss as a third-grade student and his teacher J. G. Büttner. Gauss discovered a very clever proof of the formula: $1 + 2 + 3 + \cdots + n = n(n + 1)/2$.

B. The "Prince of Mathematics."

1. Today Gauss is considered one of the greatest mathematicians ever.
2. Gauss's passion toward number theory was clear. He believed that basic relationships between numbers were fundamental to all matter. He once wrote that "God does arithmetic," and is credited with having said, "Mathematics is the queen of the sciences, and number theory is the queen of mathematics."
3. Gauss was later crowned the "Prince of Mathematics."
4. He was a perfectionist, and thus his accomplishments were much more numerous than his publications. One of his mottos was: "Few, but ripe."
5. Another favorite motto of Gauss's came from Shakespeare's *King Lear*: "Thou, nature, art my goddess; to thy laws my services are bound ... ."

II. Triangular numbers.

A. A geometric pattern of numbers.

1. The sum of the first n natural numbers is called the n^{th} *triangular number.*
2. The first few triangular numbers are 1, 3, 6, 10, 15, 21, and 28.
3. These numbers are called *triangular* because they represent the number of billiard balls that can be arranged into an equilateral triangle. Notice that the fourth triangular number, 10, revered by the Pythagoreans, equals the number of billiard balls used in a game of pool or the number of pins used in bowling.
4. Applying Gauss's elementary school formula, we see that 5050 balls are required to make a triangle with a base of 100 balls.
5. We can use the triangles to find the sum formula.

B. Turning triangles into squares.

1. In an attempt to find structure within these numbers, we consider the sums of two consecutive triangular numbers.

2. The first few of those sums equals 4, 9, 16, 25, 36, and 49. We cannot help but see a surprising pattern—the sums are perfect squares.
3. We can establish that this observation is a theorem that holds in general.
4. This result can be proven algebraically or geometrically.

C. Gauss's great theorem.

1. On July 10, 1796, at the age of 19, Gauss proved that every natural number is the sum of at most three triangular numbers. For example: $17 = 1 + 6 + 10$, and $100 = 45 + 55$.
2. He stated this result in his diary as "Eureka! Num = $\Delta + \Delta + \Delta$." In fact, Pierre de Fermat asserted this result back in 1638. He claimed to have a proof of this result, but no such proof has ever been found.
3. Establishing this result is an extremely challenging proposition. Given a natural number N, we must find whole numbers x, y, and z that satisfy the Diophantine equation $x^2 + y^2 + z^2 + x + y + z = 2N$, and this foreshadows our explorations into finding solutions to such equations later in our course.

III. A "shaky" application.

A. A hand-shaking question.

1. Suppose that a group of people assemble for a meeting. Before the proceedings begin, each pair of people shakes hands exactly once. How many handshakes are there?
2. With two people we have 1 handshake; with three people we have 3 shakes; with four people we have 6 shakes; with five people we have 10 shakes.
3. We discover that the number of handshakes will be a triangular number.
4. While this application might appear frivolous, such counting issues have applications in networking. If n computers are to be directly connected with each other, then the number of connections would be exactly the n^{th} triangular number.

B. A sample of combinatorial number theory. Counting complex scenarios is challenging, and that area of mathematics is known as *combinatorics*. The handshake question is an example of what is known as *combinatorial number theory.*

IV. The notion of arithmetic progressions.

A. Extending triangular numbers.

1. The triangular numbers arose from adding the numbers from the very simple progression 1, 2, 3, 4, 5, and so forth.

2. What feature makes the progression of natural numbers so simple? To generate the next number on our list, we merely add 1 to the previous number.

3. We can now generalize this feature. Consider the progression that starts with 1, and to generate the next number we add 2 to the previous number. This new progression is: 1, 3, 5, 7, 9, 11, 13, and so forth. We have produced the odd numbers.

B. An introduction to arithmetic progressions.

1. Progressions of numbers for which the next number in the list is produced by adding a fixed amount to the previous number are called *arithmetic progressions*.

2. So the lists 1, 2, 3, 4, ... and 1, 3, 5, 7, 9, ... are both examples of arithmetic progressions. In fact, the even numbers—2, 4, 6, 8, 10, ... —also form an arithmetic progression.

3. We can build any arithmetic progression just by knowing the first number together with the fixed amount to be added to create each successive number. For example, if we start with 5 and add 3 each time, then we have the arithmetic progression 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, and so forth.

C. A formula for the sum of the terms in an arithmetic progression.

1. The triangular numbers arose from adding up the first few numbers from the simple arithmetic progression 1, 2, 3, 4, and so forth.

2. We saw that $1 + 2 + 3 + \cdots + n = n(n + 1)/2$.

3. So one generalization to the triangular numbers can be found by considering the sums of the first few terms from any arithmetic progression. For example, if we return to the arithmetic progression 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, and so forth, then we can generate the list of sums of these numbers. That list would begin 5, 13, 24, 38, 55, 75, 98, and would provide one type of generalization of the triangular numbers.

4. Beyond extending the notion of triangular numbers, arithmetic progressions are one of the pillars of number theory and will prove to be extremely useful in our future explorations.

Questions to Consider:

1. Compute the sum of the first 1 million natural numbers.

2. Consider two consecutive triangular numbers, such as 3 and 6. Square each number and then subtract: $36 - 9 = 27$. Perform this with several examples. What do you notice about your answers? Make your own conjecture. (*Bonus*: Can you prove your conjecture holds in general?)

Lecture Four

Geometric Progressions, Exponential Growth

Scope: *Elementary number theory* is not a euphemism for "easy number theory." Instead it is an area of number theory that has its focus on fundamental questions about numbers, most of whose subtle answers do not involve advanced mathematical techniques. Here, with the notion of an arithmetic progression—a list of numbers generated by successive addition—fresh in our minds, we open these lectures on elementary number theory by exploring the multiplicative cousin of arithmetic progressions. These are known as *geometric progressions*—number lists generated by successive multiplication. These numbers grow at a dramatically fast rate and possess enormous structure. We will momentarily pause to consider how geometric progressions naturally appear in the world of music as a means of producing an even-tempered scale. Next we will turn to an extremely important and useful object in the study of advanced number theory: the *sum* of the terms of geometric progressions. Our exploration into these sums of numbers will include some amusing ancient stories that hold important mathematical morals. We will then extend this additive issue and consider the *endless* sum of *all* terms of certain geometric progressions and make such vexing ideas intuitive by visualizing such sums geometrically. The endless sum of a geometric progression is known as a *geometric series*. These series are fundamental in all corners of mathematics and science, especially—as we will see in future lectures—in number theory itself.

Outline

I. Geometric progressions.
  A. Introducing the notion of geometric progressions.
    1. An arithmetic progression is a list of numbers with the property that to get from any number to the next we need only add a fixed number. As we will discover as our course unfolds, these arithmetic progressions, while simple in structure, play an important role in our number theory story.
    2. Perhaps even more important are the corresponding progressions in which the addition is replaced by multiplication. These progressions are called *geometric progressions*.
    3. To generate a geometric progression, we must be given the first number and then the constant multiple (known as the *ratio*) that generates successive numbers on the list.
  B. Examples and illustrations.
    1. For example, if we start with 1 and are given the ratio of 2, then our geometric progression equals: 1, 2, 4, 8, 16, 32, 64, and so forth. It is easy to see that a generic term in this geometric progression is given by 2^n for some natural number n.
    2. The constant multiple (in the previous example, 2) is called the *ratio* because the ratio of any two consecutive terms—the larger to the smaller—always equals that fixed ratio. For example, notice that $32/16 = 2$.
    3. In general, if we start with 1 and have a ratio of r, then we would generate the geometric progression $1, r, r^2, r^3, r^4, r^5$, and so forth.
  C. A formula for the terms and exponential growth.
    1. These examples show us that a general term in a geometric progression is of the form r^n, for some whole number n.
    2. Since the varying quantity is the exponent n, we say that r^n *grows exponentially* if $r > 1$; and for $0 < r < 1$, we say r^n *decays exponentially*.
    3. If we start with 1 and consider $r = 1/2$, then we have a geometric progression that decays exponentially: 1, 1/2, 1/4, 1/8, 1/16, 1/32, … .

II. Progressions in music.
  A. Ratios of pitches.
    1. A musical interval is an *octave* if the two pitches have frequencies in a ratio of 2:1. An interval is a perfect fifth if the ratio of the frequencies of the two pitches is 3:2.
    2. For example, in modern Western music, the A above middle C has a frequency of 440 Hz. Thus, the A one octave higher has a frequency of $440 \times 2 = 880$ Hz, and the E one-fifth higher than A440 has a frequency of $440 \times 3/2 = 660$ Hz.

B. The chromatic scale.

1. In Western music, the *chromatic scale* begins at one pitch, say A, and progresses up in what are called *half steps* until it ends with the note that is one octave above the starting pitch. The pitches are derived from a progression of perfect fifths, starting with the first pitch.
2. A progression of perfect fifths is a geometric progression with $r = 3/2$. If we start at A (440 Hz), we would produce: 440, 440 $\times$ 3/2, 440 $\times$ $(3/2)^2$, 440 $\times$ $(3/2)^3$, 440 $\times$ $(3/2)^4$, 440 $\times$ $(3/2)^5$, and so forth; that is: 440, 660, 990, 1485, 2227.5, 3341.25, and so forth.
3. In order to keep the notes within the 440–880 Hz range, we divide the frequencies by 2 in order to lower the pitches so that they fall into the correct octave. This process requires us to modify our attractive geometric sequence.
4. So why do we end up with a 12-note chromatic scale? The answer to this question—which we will discover for ourselves later in the course—involves irrational numbers, and we leave it as a musical and mathematical cliffhanger for now.

III. Summing geometric progressions.

A. Seeking a pattern within a sum.

1. It will be extremely useful to find the sum of the first terms of a geometric progression, just as we saw with arithmetic progressions.
2. If we consider the geometric progression 1, 3, 9, 27, 81, … , then the list of the first five successive sums is: 1, 4, 13, 40, 121. A pattern is not immediately apparent.
3. To build intuition, we will explore a particular case with some care. If we let $S = 1 + 3 + 3^2$ (which equals 13), then $3S = 3 + 3^2 + 3^3$. Subtracting, we discover:

$$\begin{aligned} 3S &= 3 + 3^2 + 3^3 \\ -\ S &= 1 + 3 + 3^2 \\ \hline (3-1)S &= -1 + 3^3. \end{aligned}$$

4. So we find that $S = (3^3 - 1)/(3 - 1)$.
5. We can see this pattern holds for other sums. For example, applying the analogous pattern with $1 + 3 + 3^2 + 3^3 + 3^4$, we would conjecture that the sum equals $(3^5 - 1)/(3 - 1)$, which equals $(243 - 1)/2$, which equals 121, as expected.

B. Finding a formula.

1. We now generalize our example for finding the sum $1 + r + r^2 + r^3 + \cdots + r^n$, for any ratio $r \neq 1$. We call this sum S.
2. If we multiply S by r, we can align most of the terms in S with most of the terms in rS and then subtract:

$$\begin{aligned} rS &= r + r^2 + r^3 + \cdots + r^n + r^{n+1} \\ -\ S &= 1 + r + r^2 + r^3 + \cdots + r^n \\ \hline (r-1)S &= -1 + r^{n+1}. \end{aligned}$$

   Solving for S reveals that $S = (r^{n+1} - 1)/(r - 1)$.
3. Euclid derived this formula around 300 B.C.E.

C. The legend of the most "modest" mathematician.

1. A king wished to reward a loyal mathematician and asked him what he wanted.
2. The mathematician, who appeared both modest and humble, replied that if one grain of rice was placed on a square of an ordinary 8-by-8 chessboard and then two grains of rice were placed in the next square and so forth (doubling the previous amount of rice) until the last square was reached, then he would be content with the total sum of all the grains of rice.
3. The king laughed and immediately granted this small request. However the king quickly stopped laughing—for the number of grains of rice owed to the mathematician equaled the following sum of terms from a geometric progression (recall that there are 64 squares on the chessboard): $1 + 2 + 2^2 + 2^3 + 2^4 + \cdots + 2^{63}$, which by our formula (with $r = 2$ and $n = 63$) equals: $(2^{64} - 1)/(2 - 1) = 18{,}446{,}744{,}073{,}709{,}551{,}615$ grains of rice.
4. Given that a grain of rice weighs approximately 0.033 grams, this pile of rice would weigh approximately 671,023,802,629 tons.
5. Needless to say, the king was faced with two choices—either give up his entire kingdom to the mathematician or have the mathematician executed. Guess who had the last laugh?

IV. Infinite geometric series and taxes.

A. When does an infinite sum make sense?

1. We recall that $1 + r + r^2 + r^3 + \cdots + r^n = (r^{n+1} - 1)/(r - 1)$.
2. We now suppose that the ratio r is small, that is, $0 < r < 1$.
3. As n gets larger and larger, r^n is getting smaller and smaller and is approaching 0.
4. In this case we can consider the infinite sum of all the numbers in the geometric progression. This infinite sum is known as a *geometric series* and is extremely important in our study of number theory.
5. A geometric series is an infinite sum of the form $1 + r + r^2 + r^3 + \cdots$. But does such an endless sum have a numerical value?

B. Searching for a pattern.

1. If we consider the geometric series $1 + 1/2 + (1/2)^2 + (1/2)^3 + (1/2)^4 + (1/2)^5 + \cdots$ as representing lengths of line segments, then we can see geometrically this infinite series equals 2. (Recall that we are assuming that $0 < r < 1$.)
2. More generally, given that $1 + r + r^2 + r^3 + \cdots + r^n = (r^{n+1} - 1)/(r - 1)$, and r^{n+1} is approaching 0 as n gets larger and larger, we see that the infinite geometric series $1 + r + r^2 + r^3 + \cdots = 1/(1 - r)$.
3. We can check this formula for the case $r = 1/2$ and see that the infinite series equals $1/(1 - 1/2) = 1/(1/2) = 2$, as we just saw.
4. This formula for infinite geometric series will be an important and useful fact as we move into the subtle points of number theory.

C. A prize-winning application.

1. Suppose you win a million-dollar prize on a game show. At first you believe you have a million dollars to enjoy. However, Uncle Sam has other plans. He will take 1/3 of your bounty in tax.
2. However, suppose the game show desires so much hype that it offers to pay the tax for you so you will take home the full $1 million. So they pay (1 + 1/3) million dollars. However, you still do not take home a million dollars, because you now have to pay 1/3 tax on the extra 1/3 they gave you (1/9 of a million dollars).

3. If they offer the extra 1/9 of a million dollars, then that additional amount will be taxed. How much must they offer so you can take home a million dollars after taxes?
4. The answer is the infinite series: $1 + (1/3) + (1/3)^2 + (1/3)^3 + (1/3)^4 + (1/3)^5 + \cdots = 1/(1 - 1/3) = 3/2$ million dollars. We see that the tax on this amount is $3/2 \times 1/3 = 1/2$ million dollars. If we deduct this from the 3/2 million, we see that you are left with exactly 1 million dollars—after taxes.

Questions to Consider:

1. Consider the geometric progression that begins −2, −10, −50, −250. Without explicitly adding the terms themselves, determine the sum of the first five terms. (*Hint*: Notice that this progression equals the progression you get if you start with 1, 5, 25, 125, … and then multiply each term by −2.)
2. Recall that the decimal number 0.999… means 9/10 + 9/100 + 9/1000 + … . Find the *sum* of this infinite geometric series using the formula introduced in the lecture. Are you surprised that your answer equals 0.999…? (*Hint*: Notice that this progression equals the progression you get if you start with $1 + 1/10 + 1/100 + \cdots$ and then multiply each term by 9/10.)

Lecture Five

Recurrence Sequences

Scope: As we have seen in the previous two lectures, we can generate both arithmetic and geometric progressions by either adding or multiplying a fixed value to a previous term in order to produce the next term in our progression. In this lecture we will extend these ideas by studying important patterns of numbers in which the next term in our number list is found by calculating a fixed, predetermined combination of the previous terms. We will see that both arithmetic and geometric progressions are very special examples of this much more general notion of number sequence. These more intricate number patterns are known as *recurrence sequences*. The most famous recurrence sequence is the list of Fibonacci numbers and their second cousins, the Lucas numbers. Using the Fibonacci and Lucas numbers as exemplars, we will explore the structure and patterns hidden within recurrence sequences. As we study their growth, we will come upon one of the most controversial and famous numbers in human history: the golden ratio. After discovering the arithmetic aesthetics of this number, we will apply its connection with Fibonacci numbers to reveal a very clever and practical method of converting between miles and kilometers.

Outline

I. Growing sequences with a starting seed and a simple rule.
   A. Extending the ideas of arithmetic and geometric progressions.
      1. For arithmetic progressions, we generate a new value by adding a given fixed number to the previous value in the progression.
      2. For geometric progressions, we generate a new value by multiplying a given fixed number by the previous value in the progression.
      3. We notice that both arithmetic and geometric progressions are generated by the initial number, known as the *starting seed*, and the rule that produces the next number from the previous number.

   B. The notion of recurrence.
      1. We now extend this method to produce more intricate lists of numbers.
      2. Instead of the simple rule of either adding or multiplying by a fixed number to generate the next term in our sequence of numbers, we will now consider more interesting combinations of the previous terms to generate the next number.
      3. Just as with arithmetic and geometric progressions, the new generating rule involving the previous numbers from our sequence will remain the same as we produce our list of numbers.
      4. Such sequences of numbers—number lists in which terms in the sequence are found by applying a fixed rule involving the numbers that came before—are called *recurrence sequences*.
   C. The whole story from two pieces of information.
      1. As we have seen with both arithmetic and geometric progressions, a recurrence sequence can be described precisely by just giving the first few terms (the starting seeds) and then the fixed rule that generates the next number.
      2. Thus only two pieces of information are required to define a recurrence sequence: the starting seeds and the generating rule.
      3. So arithmetic and geometric progressions are each examples of recurrence sequences.

II. Patterns within the sums of Fibonacci and Lucas numbers.
   A. Two important illustrations.
      1. We now consider some concrete examples of recurrence sequences that are neither arithmetic nor geometric progressions.
      2. We fix our generating rule to be: Add two consecutive numbers to produce the next term in the sequence.
      3. We still require starting seeds. In this case, we need two numbers to allow our process to start.
      4. Suppose that our starting seeds are 1 and 1. So the first two terms in our sequence are 1, 1, and the process to generate the next term is always the same—add the previous two numbers.

5. In this case our recurrence sequence is 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, and so forth. This famous sequence is known as the *Fibonacci numbers*, named after the 13th-century Italian mathematician Leonardo de Pisa (also known as Fibonacci). These numbers appear in unexpected places, including nature and art. They will make cameo appearances throughout our course.
6. We can generate a different recurrence sequence by simply changing the starting seeds (but keeping the same rule of adding two adjacent numbers to generate the next number). Suppose we start with 2 and 1.
7. This new recurrence sequence begins 2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, and so forth. This sequence is called the *Lucas sequence*, named after the 19th-century French mathematician Edouard Lucas.

B. Hidden patterns within the sequences.

1. As we march through these sequences of numbers, the two appear to have nothing in common. However, they do share the same generating rule, so perhaps there is some hidden connection.
2. If we sum pairs of Fibonacci numbers that are two apart from each other we see: $1 + 2 = 3$; $1 + 3 = 4$; $2 + 5 = 7$; $3 + 8 = 11$. Incredibly, we discover the Lucas sequence.
3. The idea of the inductive proof of this theorem can be seen by considering $3 + 8$ and first writing each as the sum of two adjacent Fibonacci numbers: $3 + 8 = (1 + 2) + (3 + 5) = (1 + 3) + (2 + 5) = 4 + 7$, which is the sum of two adjacent Lucas numbers. Therefore this sum equals the next Lucas number, 11.
4. As before with the progressions we studied, we can consider the sum of the first terms of the Fibonacci or Lucas sequences. If we compute cumulative sums of the first terms of the Fibonacci sequence, we obtain: 1, 2, 4, 7, 12, 20, 33, and so forth. What do we see?
5. If we add 1 to each number on our list, we return to the Fibonacci sequence: 2, 3, 5, 8, 13, 21, 34, and so forth. Can this "magic" be explained by mathematics?

6. We can use a "domino idea": We consider a sum of Fibonacci numbers but add 1 at the beginning. That additional 1 generates a chain reaction of consecutive Fibonacci numbers:

$$\begin{aligned} & 1 + 1 + 1 + 2 + 3 + 5 \\ &= 2 + 1 + 2 + 3 + 5 \\ &= 3 + 2 + 3 + 5 \\ &= 5 + 3 + 5 \\ &= 8 + 5 \\ &= 13. \end{aligned}$$

7. A similar result holds for the Lucas sequence as well.

III. Measuring the growth of recurrence sequences of numbers via ratios.

A. Since the term we add to a Fibonacci number to generate the next one is increasing, we know that the Fibonacci sequence is *not* an arithmetic progression. But perhaps the Fibonacci sequence is a geometric progression.

B. This issue inspires us to examine the *ratios* of consecutive Fibonacci numbers.

1. $1/1$; $2/1 = (1 + 1)/1 = 1 + 1/1$; $3/2 = (2 + 1)/2 = 1 + 1/2 = 1 + 1/(1 + 1/1)$; $5/3 = (3 + 2)/3 = 1 + 2/3 = 1 + 1/(1 + 1/(1 + 1/1))$.
2. Thus we see that while the Fibonacci sequence is not a geometric progression, the ratios of consecutive terms *are* approaching a number: An endless fraction-within-fraction of the form $1+ 1/(1+ 1/(1 + 1/(1+ 1/(1 + 1/(1 + 1/(1+ 1/(1 + 1/(1 + 1/(1 \cdots$.
3. This number is called the *golden ratio*.

IV. The golden ratio.

A. A continued fraction.

1. This representation of the golden ratio as an endless fraction-within-fraction is an example of a *continued fraction*, which we will study at the end of this course. Thus this number foreshadows our number travels to come.
2. We now wonder if the golden ratio can be expressed as a more familiar-looking number.

B. A self-similar number.

1. We notice that if we call the golden ratio φ [phi] then we realize that $\varphi = 1 + 1/\varphi$.

2. Solving this equation is equivalent to solving the quadratic equation $\varphi^2 - \varphi - 1 = 0$.
3. Using the quadratic formula, we find two solutions: $(1 + \sqrt{5})/2$ and $(1 - \sqrt{5})/2$. Since the second solution is negative and φ is positive, we discover that $\varphi = (1 + \sqrt{5})/2$.
4. The decimal expansion for φ is 1.618033989..., which hides much of the structure of φ that we already uncovered.

C. Aesthetics and beauty within number.

1. While φ is one of the most famous numbers, it is also one of the most controversial. Many believe that the golden ratio appears in nature and art and informs our aesthetic tastes. Others disagree.
2. It is a fact that the golden ratio does appear in many different areas of number theory, mathematics, and science.
3. It is also a fact that the golden ratio is the only number that can be expressed as an endless continued fraction consisting solely of 1s.
4. We will return to the golden ratio and see that even though it is an irrational number, it is the "least" irrational number that exists. Thus within the world of number theory, it is difficult to argue that φ is not an abstract object of great importance and beauty.

D. Using φ today in our everyday travels.

1. We close this lecture with a practical application of the Fibonacci numbers and their connection with the golden ratio.
2. The golden ratio equals 1.618..., which coincidentally is extremely close to the number of kilometers that equals a mile. In fact, 1 mile = 1.6093... kilometers.
3. We can use the Fibonacci numbers to convert between kilometers and miles.
4. To illustrate the method, we will approximate the number of miles in a 10-km run. First we express 10 as a sum of Fibonacci numbers: 10 = 2 + 8. Next we replace each Fibonacci number in our sum with the Fibonacci number that precedes it in the Fibonacci sequence. In this case we replace 2 + 8 by 1 + 5, which equals 6. Therefore 10 km is approximately 6 miles (in fact, it is about 6.2 miles). How many miles is a 50-km trip? We write 50 = 34 + 13 + 3 and then compute 21 + 8 + 2 = 31 miles (actual mileage is 31.06...).

Questions to Consider:

1. a) Without adding them directly, determine the sum of the first 10 Fibonacci numbers.

   b) Use the Fibonacci sequence to find the number of kilometers roughly equivalent to 100 miles. (*Hint*: First write 100 as the sum of Fibonacci numbers.)
2. Look at attractive rectangular shapes around you. For each one, compute the ratio of the longer side to the shorter side. Are any of your ratios close to the golden ratio?

Lecture Six

The Binet Formula and the Towers of Hanoi

Scope: Beyond their intrinsic appeal and utility to number theorists, recurrence sequences of numbers are important objects of computer science. The question of considerable interest is, Can we find a formula that will produce any individual term in this sequence of numbers without the need for generating *all* the numbers in the list up to that term? In this lecture we will tackle this challenge by discovering the famous Binet formula for the Fibonacci numbers. While named after the French mathematician Jacques Binet who first derived it in 1843, it appears that this important formula was apparently known to Leonhard Euler and Daniel Bernoulli over 100 years earlier. Once we derive this formula, by separating a pattern we will realize that our method can be generalized and used to find corresponding formulas for all such recurrence sequences. The Binet formula will provide us with the insight that while recurrence sequences such as the Fibonacci and Lucas numbers are not geometric progressions, they are in fact a combination of two geometric progressions. We will then close this lecture with one of the most famous stories involving recurrence sequences of numbers: The Towers of Hanoi.

Outline

I. The practical importance of recurrence sequences.

A. A world of recurrence.

1. In the previous lecture we discovered recurrence sequences: lists of numbers that can be generated using some starting seeds (the first few numbers) and a rule for generating future numbers.

2. Arithmetic and geometric progressions are very simple examples of recurrence sequences, as are the Fibonacci and Lucas sequences.

B. An important idea within computer science.

1. A recurrence relation is one in which previous information is used in a systematic manner to generate new information.

2. The concept of recurrence is an important and fundamental component in many computer algorithms and languages.

3. As a result, all computer scientists have studied and use recurrence sequences in their programming.

II. Finding a "closed formula" for the Fibonacci numbers.

A. A recurrence definition versus a formula.

1. Suppose we let F_n denote the n^{th} Fibonacci number. So we have $F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3, F_5 = 5, F_6 = 8, F_7 = 13$, and so forth.

2. This notation allows us to precisely define the recurrence rule as $F_{n+1} = F_n + F_{n-1}$, for all $n \geq 2$.

3. One disadvantage to describing the Fibonacci numbers in this manner is that if we wish to find the value of the 1000^{th} Fibonacci number we would be required to compute all the previous ones in succession and work our way to the 1000^{th} one.

4. Ideally we would like a "closed formula"—that is, a generic formula in which we can just plug in 1000 to produce the 1000^{th} Fibonacci number without computing any others.

5. One of the important features of many recurrence sequences, in general, is that such closed formulas can be derived, and we will illustrate this process with the Fibonacci numbers.

B. A focus on φ.

1. We recall that in our attempt to express φ in a more familiar form (rather than as a continued fraction), we saw that φ was one of the solutions to $x^2 = x + 1$.

2. Using the quadratic formula we found that the two solutions to this equation are $(1 + \sqrt{5})/2$ and $(1 - \sqrt{5})/2$. Because φ is a positive number, we found that $\varphi = (1 + \sqrt{5})/2$. We now write τ for the negative solution, that is, $\tau = (1 - \sqrt{5})/2$.

3. Since both φ and τ are solutions to the equation, we see that $\varphi^2 = \varphi + 1$ and $\tau^2 = \tau + 1$.

4. We can use the formula $\varphi^2 = \varphi + 1$ to simplify φ^3: $\varphi^3 = \varphi\varphi^2 = \varphi(\varphi + 1) = \varphi^2 + \varphi = (\varphi + 1) + \varphi = 2\varphi + 1$. So we see that $\varphi^3 = 2\varphi + 1$.

C. Discovering a pattern.

1. We apply the same technique to find φ^4: $\varphi^4 = \varphi\varphi^3 = \varphi(2\varphi + 1) = 2\varphi^2 + \varphi = 2(\varphi + 1) + \varphi = 3\varphi + 2$.

2. Similarly for φ^5: $\varphi^5 = \varphi\varphi^4 = \varphi(3\varphi + 2) = 3\varphi^2 + 2\varphi = 3(\varphi + 1) + 2\varphi = 5\varphi + 3$.
3. Finally we find $\varphi^6 = \varphi\varphi^5 = \varphi(5\varphi + 3) = 5\varphi^2 + 3\varphi = 5(\varphi + 1) + 3\varphi = 8\varphi + 5$, and a pattern emerges.
4. We summarize our findings:

$$\varphi^2 = \varphi + 1$$
$$\varphi^3 = 2\varphi + 1$$
$$\varphi^4 = 3\varphi + 2$$
$$\varphi^5 = 5\varphi + 3$$
$$\varphi^6 = 8\varphi + 5.$$

5. We see the Fibonacci numbers appearing. In fact we can continue this process indefinitely and thus conclude that in general for any natural number n, $\varphi^n = F_n\varphi + F_{n-1}$.
6. By the identical reasoning, since τ is also a solution to $x^2 = x + 1$, we see that a corresponding amazing formula holds for τ. That is, for any natural number n, $\tau^n = F_n\tau + F_{n-1}$.
7. If we now subtract these two formulas, we see:

$$\begin{aligned} \varphi^n &= F_n\varphi + F_{n-1} \\ -\ \tau^n &= F_n\tau + F_{n-1} \\ \hline (\varphi^n - \tau^n) &= F_n(\varphi - \tau) + 0. \end{aligned}$$

8. We can now solve this equation for F_n and find that for all n, $F_n = (\varphi^n - \tau^n)/(\varphi - \tau)$.
9. We note that $\varphi - \tau = (1 + \sqrt{5})/2 - (1 - \sqrt{5})/2 = \sqrt{5}$, and thus we have derived a closed formula for the n^{th} Fibonacci number: $F_n = (\varphi^n - \tau^n)/\sqrt{5}$. This elegant formula today is known as the *Binet formula*, named after the 19th-century French mathematician Jacques Binet.
10. The 1000th Fibonacci number equals $(\varphi^{1000} - \tau^{1000})/\sqrt{5}$, which a computer can simplify to the 209-digit Fibonacci number:

43466557686937456435688527675040625802564660517371780402481729089536555417949051890403879840079255169295922593080322634775209689623239873322471161642996440906533187938298969649928516003704476137795166849228875.

D. Nearly a geometric progression.
   1. Recall that we found that the Fibonacci sequence is not a geometric progression since the ratio of consecutive terms is not constant.
   2. We did see that those ratios are converging on a particular value. The value the ratios are approaching is the golden ratio, φ.
   3. Using Binet's formula, we now discover that the Fibonacci numbers are, in fact, the difference of two geometric progressions.

E. Lucas numbers revealed.
   1. Applying our previous analysis with the Lucas sequence, we can derive the closed formula: For all $n > 1$, $L_n = \varphi^{n-1} + \tau^{n-1}$.
   2. In fact, the terms in any recurrence sequence can be expressed as a closed formula.

III. The legend of the Towers of Hanoi.

A. The history of a towering tale.
   1. "The Towers of Hanoi" was a logic puzzle that was marketed in 1883 by a "Professor Claus." However, "Professor Claus" is, in fact, an anagram of its true inventor, Professor Lucas.
   2. The Towers of Hanoi puzzle consists of three pegs and a collection of punctured disks of different diameters that can be placed on the pegs.
   3. The puzzle begins with all the disks on one peg in order of diameter, with the largest disk on the bottom.
   4. The object is to transfer all the disks to another peg so that they end up residing on this new peg in the original descending order. The rules are: Only one disk can be moved from one peg to another at a time, and at no time can a larger disk be placed on top of a smaller disk.
   5. Our challenge is to find a method for moving the disks and to determine the number of moves required.

B. A towering recurrence.
   1. Suppose we have n disks to be moved. We begin by observing that to move the largest (very bottom) disk, we must first move the other $n - 1$ smaller disks.
   2. Once we move those $n - 1$ disks to a new peg, then we can remove the last, largest disk and move it to the remaining

empty peg. Now we must move the other $n - 1$ smaller disks back on top of the largest one.

3. Let us write h_n for the number of moves required to move n disks. We now wonder if we can find a recurrence rule that generates the sequence of h_n's.

C. Discovering a pattern.

1. By experimenting we can see that $h_1 = 1$, $h_2 = 3$, and $h_3 = 7$.
2. In view of the disk-moving process, h_n must equal $h_{n-1} + h_{n-1} + 1$, that is, we have the recurrence rule: $h_n = 2h_{n-1} + 1$.
3. So the number of moves required for 4 disks equals $2 \times 7 + 1$, which equals 15.
4. We can find a closed formula by looking at our sequence of h_n's: 1, 3, 7, 15. We notice that each number is one less than a power of two: $1 = 2 - 1$, $3 = 2^2 - 1$, $7 = 2^3 - 1$, and $15 = 2^4 - 1$.
5. In general, it is possible to prove that $h_n = 2^n - 1$, which gives a simple closed formula for the number of disk moves required if we have n disks.

D. Determining the end of the world.

1. There is a legend that a certain group of monks had a particularly impressive edition of this puzzle consisting of 64 gold disks and three diamond pegs. They were able to move 1 disk per second.
2. The legend is that the world would end once the monks completed their mission. We can now employ the closed formula we just found to predict when the world will end.
3. The number of moves required to solve this puzzle with 64 disks equals $2^{64} - 1$. Given that the monks move the disks at a rate of one disk per second, this number of moves would take 583,344,214,028 years, and thus it would take that many years for the world to end.
4. The optimal solution for the Towers of Hanoi with four pegs remains an open question.

Questions to Consider:

1. Here are the first few terms of a recurrence sequence. Can you find the rule that generates the next term using one or more previous terms?

   1, 1, 4, 13, 43, 185, ...

2. Suppose there are 10 disks in your Towers of Hanoi puzzle. Use the method outlined in the lecture to compute how many moves are required to move all the disks to a new peg.

Lecture Seven

The Classical Theory of Prime Numbers

Scope: Here we introduce the ideas that feed analytic number theory—the study of prime numbers. The main goal of this classical area of study is to uncover the distinctive personalities of natural numbers through the arithmetic structure that unfolds from multiplicative considerations—specifically, from expressing natural numbers as products of the smallest possible factors greater than 1. This factorization idea will allow us to partition the natural numbers greater than 1 into two disjoint collections—the prime numbers and the composite numbers. We will discover why 1 is neither prime nor composite—an issue that will also foreshadow the birth of algebraic number theory. In this lecture we will discover the 2000-year-old struggle to understand the primes that started in ancient Greece with important contributions by Euclid and Eratosthenes. Along the way, we will encounter the fundamental theorem of arithmetic and establish this important result through a "divide and conquer" argument. We will also see how to create a "sieve" to sift out the primes from the composite numbers and then discover that there are, in fact, infinitely many prime numbers. Euclid established this result, which is considered to be one of the most elegant proofs in mathematics. Finally, armed with the reality that there are infinitely many primes, we wonder if the prime numbers appear with any regularity within the natural numbers.

Outline

I. The story of the prime numbers.

A. The basic building blocks of number theory.

1. How can we generate the natural numbers? There are several different methods involving addition.

2. The simplest is to start with 1 and continue to add 1 repeatedly. In fact, this is the simplest example of an arithmetic progression.

3. If we start with the triangular numbers as building blocks, then we could apply Gauss's profound result that he discovered at the age of 19: Every natural number is the sum of at most three triangular numbers.

4. Alternatively, in our discussion of Fibonacci numbers we outlined a method for converting kilometers to miles. Implicit in that method is the fact that every natural number can be written as the sum of distinct Fibonacci numbers.

5. Here we will consider the basic multiplicative building blocks of the natural numbers.

B. Factorization as a personality trait of numbers.

1. To understand the arithmetic structure and individuality of the natural numbers better, we study their basic components when viewed as products of smaller numbers.

2. The process of expressing natural numbers as products of smaller numbers is known as *factoring*. The terms in the product are called *factors*.

3. The individual factors reveal features of the number. For example, if a number has a factor of 2, then it must be even. If a number has a factor of 10, then the number's last digit must be 0.

C. A brief history of the primes.

1. We define the prime numbers to be the atoms of the natural numbers—those that cannot be split into smaller pieces. More precisely, a natural number greater than 1 is called *prime* if it cannot be expressed as the product of two smaller natural numbers.

2. The first few primes are 2, 3, 5, 7, 11, 13, 17, 19, and 23. The number 6 is not prime because it can be written as 2×3. Similarly, 15 is not prime since it equals 3×5. Numbers that are greater than 1 and not prime are called *composite numbers*.

3. Euclid, around 300 B.C.E., was the first to embark upon a rigorous and formal study of the prime numbers and some of the properties they possess.

II. The unique factorization property.

A. Euclid's *Elements*.

1. Euclid's *Elements of Geometry*—a series of 13 books many consider to be some of the most important treatises ever

written—contain approximately 100 important results involving number theory.

2. Two of his results—which we will now explore—are the cornerstones for the two main branches of number theory.

B. A unique factorization property.

1. The first theorem of Euclid that we highlight here is what is now known as the *fundamental theorem of arithmetic*, which in essence asserts that the primes are indeed the multiplicative building blocks of all natural numbers greater than 1.
2. The fundamental theorem of arithmetic: Every natural number greater than 1 can be expressed uniquely as a product of prime numbers.
3. For example, 12 can be expressed as $2 \times 2 \times 3$, and except for rearrangement of these prime factors, this prime factorization is unique. Thirteen is a prime so we would write it as the "product" 13, again in only one way.

C. A "divide and conquer" argument.

1. The argument that established the validity of the fundamental theorem of arithmetic involves the technique of "divide and conquer."
2. Suppose we are given a natural number $n > 1$. If it is a prime number, then we have factored it into primes and we are done. If n is not a prime (so it is composite), then by definition it can be expressed as the product of two smaller natural numbers.
3. We now repeat this process with each of the two smaller factors. This process will eventually terminate; that is, we will not be able to factor the numbers any further. In other words, we are left only with prime factors, as desired.
4. Verifying the uniqueness of the factorization into primes is much more subtle, although intuitively it seems reasonable. We will return to this uniqueness of factorization into primes in our excursion into algebraic number theory, in particular, in Lecture Fifteen.
5. This uniqueness property also helps us understand why we do not consider 1 a prime number. If it were prime, then we would not have unique factorization; for example, $6 = 2 \times 3 = 1 \times 2 \times 3$.

III. The Sieve of Eratosthenes.

A. Eratosthenes and his work.

1. Given that the primes are the fundamental multiplicative building blocks for the natural numbers, early on in the human history of number theory there was a desire to identify which numbers are primes.
2. Around 200 B.C.E., Eratosthenes discovered a method for taking the natural numbers and "sifting" out the composite numbers. Thus his "sieve," now known as the *Sieve of Eratosthenes*, collected all the prime numbers up to any particular value.

B. Sifting out the composite numbers.

1. Suppose we wish to list all the primes less than 100. Eratosthenes's method is to write all the numbers from 2 through 100. We start at the first number, 2, and from there we cross every other number off our list. In this case, we would cross off 4, 6, 8, 10, and so forth; all the even numbers, except 2, would be crossed off.
2. We move to the next number not crossed off our list, in this case, 3. From there we cross off every third number (with the understanding that we might be crossing off numbers that have already been removed). In this case, we remove all the multiples of 3: 6, 9, 12, 15, 18, and so forth.
3. If we repeat this process, then when we are finished, the only numbers *not* crossed off are precisely all the prime numbers less than 100.
4. It might appear as if there are a large number of steps required to get all these primes. However, Eratosthenes showed that we need only repeat this pruning process up to the square root of 100, which is 10. That is, we need only perform four steps (one for each prime less than 10: 2, 3, 5, and 7) to generate *all* the primes up to 100!

C. Why this sieve works so quickly.

1. Initially it seems surprising that we need only four steps to generate all the primes up to 100.
2. We need to prove that after we sieve out by all the numbers up to 10, the numbers beyond 10 that have *not* been sifted out are all primes. We will establish this assertion by assuming the opposite and producing a contradiction.

3. Suppose that there were a composite not crossed off our list. Then it is not a multiple of any number less than or equal to 10, so it is the product of two numbers greater than 10. Thus it is greater than 10×10, or 100, which is too large to appear on our list.
4. Therefore we see that there cannot be any composite numbers left beyond 10.
5. In general, if we wish to find all the primes up to n, we need only sieve up to $\sqrt{n}$.

D. A larger example.

1. Suppose we wanted to list all the primes less than 500.
2. This at first appears to be a daunting task. However we note that $\sqrt{500} = 22.3606\ldots$, so all we need to do is list the natural numbers from 2 to 500 and repeat this sieving process until we reach 22.
3. It is easy to check that the complete list of primes less than 22 is 2, 3, 5, 7, 11, 13, 17, and 19. Thus just after eight sifting processes, we will have generated *all* the primes up to 500!

IV. How many primes are there?

A. Euclid's result on the infinitude of primes.

1. Inspired by Eratosthenes's sieve, we now wonder how many primes there are.
2. This brings us to the second theorem of Euclid that we celebrate in this lecture. In Book IX of his *Elements of Geometry*, Proposition 20 states: Prime numbers are more than any assigned multitude of prime numbers.
3. Today we would state this assertion as: There are infinitely many prime numbers.
4. This extremely important 2300-year-old result of Euclid's is the pillar upon which analytic number theory was built. We will study the later refinements of this theorem in the next lecture.
5. However, here we will follow Euclid's ingenious proof that establishes this great theorem.

B. Searching for a prime greater than 3.

1. To build our intuition, we first begin simply: How can we find a prime beyond 2 and 3?

2. One method is to announce, "5," and move on, but this method does not easily generalize.
3. Another approach is to first consider the number 2×3. Of course this number is certainly not prime, since it is the product of both 2 and 3. However Euclid's clever idea is to add 1; that is, he considered the number $2 \times 3 + 1$ and argued that any prime dividing this number cannot be 2 or 3.
4. Thus Euclid proved there exists a prime beyond 3 without using the fact that 3 is a specific small prime. Euclid's devilishly clever idea can be extended to prove his theorem in general.

C. Euclid's beautiful proof.

1. Let $p_1, p_2, p_3, \ldots, p_n$ be the first n prime numbers. Our goal is to prove that there must exist another prime not on this list.
2. We remark that each of the first n prime numbers divides evenly into the product of all of them: $p_1 \times p_2 \times p_3 \times \cdots \times p_n$.
3. Euclid then considers the number $E = p_1 \times p_2 \times p_3 \times \cdots \times p_n + 1$. Now, E is a natural number greater than 1, so we know by the fundamental theorem of arithmetic that it can be factored into primes. Let us say that q is one of the prime numbers that divide evenly into E.
4. Can the prime q be one of the first n prime numbers? Since E is the product of the first n primes plus 1, we see that none of these n primes can divide evenly into E. When we divide any of those primes into E, we find a remainder of 1.
5. Thus q must be a prime number that is not contained in the first n primes. Therefore we conclude that there are more than n primes—and since n was an arbitrary number, there must be infinitely many primes.
6. Most mathematicians view Euclid's proof as one of the most elegant arguments in all of mathematics.

V. Are there long runs of composite numbers?

A. Runs of composite numbers.

1. We have seen that there are infinitely many prime numbers and infinitely many composite numbers.
2. We cannot have two consecutive numbers both being prime beyond 2 and 3, since every other number is even (and thus has a factor of 2).

3. Can we find two consecutive numbers both of which are composite? Yes: 8 and 9 is the smallest such pair. In fact, 8, 9, 10 is a run of three consecutive composite numbers. We note that 24, 25, 26, 27, and 28 is a run of five consecutive composite numbers.

B. What is the maximum run of consecutive composite numbers before hitting a prime?

1. It is a theorem that there are arbitrarily large runs of composite numbers. That is, given any natural number N, there exists a run of N consecutive composite numbers.
2. Phrased differently, given any natural number N, two prime numbers exist whose distance from each other is at least N and for which there are no other prime numbers between them.
3. More informally, we can find arbitrarily long runs of natural numbers that are deserts free of primes—there are none to be found!

C. A modification of Euclid's argument.

1. To prove the assertion that given any natural number N there exists a run of N consecutive composite numbers, we invoke a clever modification of Euclid's method of proving there are infinitely many primes.
2. We start with the number K, defined to be the product of the natural numbers given by $K = 2 \times 3 \times 4 \times \cdots \times (N+1)$. We observe that K is divisible by all the numbers from 2 to $N+1$. (Note that there are N numbers in this list of divisors.)
3. We now consider $K + 2 = 2 \times 3 \times 4 \times \cdots \times (N+1) + 2$. The number $K + 2$ is divisible by 2 and therefore is composite.
4. The next number, $K + 3$, equals $2 \times 3 \times 4 \times \cdots \times (N+1) + 3$, and we note that this number is also composite, because 3 is a factor of $K + 3$. Similarly, we see that 4 is a factor of $K + 4$, so it is composite.
5. This pattern continues all the way through the number $K + (N+1)$, which is composite because $N + 1$ is a factor of $2 \times 3 \times 4 \times \cdots \times (N+1) + (N+1)$.
6. Thus we see that each of the N consecutive numbers, $K + 2, K + 3, \ldots$, and finally $K + (N+1)$, is composite. So we found a run of at least N consecutive composite numbers.
7. This argument is effective in that it gives a method for finding the run of numbers, although it is not practical for long runs.

8. By creating a variation on Euclid's theme, we were able to produce an entirely new result.

Questions to Consider:

1. Using the method of Euclid and the prime numbers 2, 3, 5, 7, 11, 13, 17, and 19, explicitly describe a natural number that contains a prime factor greater than 20.
2. Describe a number that is itself composite and for which the next 1 million consecutive natural numbers are all composite numbers.

Lecture Eight

Euler's Product Formula and Divisibility

Scope: We will open this lecture by deriving what is arguably the most important formula involving prime numbers. In particular, we will connect an endless product involving the primes with the endless sum of the reciprocals of natural numbers: $1/1 + 1/2 + 1/3 + 1/4 + \cdots$. The derivation of this formula will involve our previous work on geometric series. This fundamental identity, first found by Leonhard Euler, will lead us to a "modern" proof that there are infinitely many primes. We will then see that while Euclid's ancient proof of the infinitude of primes is considered to be one of the most aesthetically appealing arguments in mathematics, Euler's analytic proof led naturally to the dawn of modern analytic number theory. While we address the true importance of Euler's formula and its generalizations in the lecture that follows this one, here we will explore how his formula allows us to analyze subtle questions involving divisibility of generic or randomly selected natural numbers. These questions are delicate and have a probabilistic feel to them. In particular, we will determine the likelihood that a natural number selected at random will have no repeated prime factors and, through our analysis, experience for ourselves the power of Euler's remarkable formula.

Outline

I. A formal formula of Euler's.
  A. Euler's amazing product formula.
    1. Leonhard Euler, an 18th-century Swiss mathematician, was one of the most prolific and important mathematicians in history.
    2. In 1737, he discovered a formula that gave birth to modern analytic number theory.
    3. This formula shows that a certain product involving prime numbers equals a certain sum of fractions.
    4. Euler's formula states that $(1/(1 - 1/2)) \times (1/(1 - 1/3)) \times (1/(1 - 1/5)) \times (1/(1 - 1/7)) \times (1/(1 - 1/11)) \times \cdots = 1 + 1/2 + 1/3 + 1/4 + 1/5 + 1/6 + \cdots$.

    5. So Euler's product formula asserts that if we multiply $1/(1 - 1/p)$ for every prime number p, then the result will be the sum of the reciprocals of all the natural numbers.
    6. We will now see why such a formula is believable by manipulating the product to equal the endless sum. We will treat both of these expressions as formal objects; that is, we will not wonder if these expressions represent actual numbers.

B. Returning to geometric infinite series.
  1. We return to the formula we derived for geometric infinite series: For any number r satisfying $0 < r < 1$, we found that the endless sum $1 + r + r^2 + r^3 + r^4 + \cdots$ equals $1/(1 - r)$.
  2. This is the key formula that will allow us to see why Euler's product formula is believable.
  3. For any prime number p, we notice that $1/p$ is positive and less than 1 ($0 < 1/p < 1$). The numbers we are multiplying together in Euler's formula are of the form $1/(1 - 1/p)$, so we now have a crucial insight: Numbers of that form are the sum of an infinite geometric series!
  4. Specifically, we note that $1 + (1/p) + (1/p)^2 + (1/p)^3 + (1/p)^4 + \cdots = 1/(1 - 1/p)$.

C. A crash course in multiplication.
  1. We now focus on the product in Euler's product formula and replace each term by its equivalent infinite geometric series.
  2. We find: $(1/(1 - 1/2)) \times (1/(1 - 1/3)) \times (1/(1 - 1/5)) \times \cdots = (1 + (1/2) + (1/2)^2 + (1/2)^3 + \cdots) \times (1 + (1/3) + (1/3)^2 + (1/3)^3 + \cdots) \times (1 + (1/5) + (1/5)^2 + (1/5)^3 + \cdots) \times \cdots$.
  3. To multiply these geometric series together, we pluck out one term from each sum and multiply those terms together. We then add up all the products we get from all the different ways of plucking one term from each geometric series.
  4. For example, if we select 1 from each series, then that product of 1s equals 1. If we select 1/2 from the first series and 1s from the others, then that product equals 1/2. If we select 1 from the first series, 1/3 from the second series, and 1s from the rest, then that product equals 1/3.
  5. Will we find 1/4? Yes—we select 1/4 from the first series and 1s from the rest. How about 1/5? Sure—select 1 from the first and second series, pluck out 1/5 from the third series, and 1s

from the rest. How about 1/6? Yes, but this is a bit trickier: We pluck 1/2 from the first series, 1/3 from the second series, and 1s from the rest. That product yields 1/6.

6. Because we have all the powers of all the primes, then by the fundamental theorem of arithmetic we know that this process will produce all numbers of the form $1/n$ for all natural numbers n and that the reciprocal will only appear once in our sum.
7. For example, how would we find 1/300? We would pluck 1/4 from the first series, 1/3 from the second series, 1/25 from the third series, and 1s from the rest.
8. Thus we see that Euler's product formula, $(1/(1 - 1/2)) \times (1/(1 - 1/3)) \times (1/(1 - 1/5)) \times (1/(1 - 1/7)) \times (1/(1 - 1/11)) \times \cdots = 1 + 1/2 + 1/3 + 1/4 + 1/5 + 1/6 + \cdots$, makes sense. We caution that we are not claiming that either the endless product on the left or the endless sum on the right has actual numerical values.

D. Euler's general product formula.

1. In fact we can apply the same reasoning to verify a more general product formula due to Euler. Namely, for any number s, $(1/(1 - 1/2^s)) \times (1/(1 - 1/3^s)) \times (1/(1 - 1/5^s)) \times (1/(1 - 1/7^s)) \times (1/(1 - 1/11^s)) \times \cdots = 1 + 1/2^s + 1/3^s + 1/4^s + 1/5^s + 1/6^s + \cdots$.
2. The infinite series $1 + 1/2^s + 1/3^s + 1/4^s + 1/5^s + 1/6^s + \cdots$ is now known as the *zeta function* and is written as $\zeta(s) = 1 + 1/2^s + 1/3^s + 1/4^s + 1/5^s + 1/6^s + \cdots$.

II. A modern proof of the infinitude of primes.

A. The perplexing *harmonic series*.

1. Now that we have established Euler's product formula, we ask, what good is it?
2. The series $1 + 1/2 + 1/3 + 1/4 + 1/5 + 1/6 + \cdots$ is known as the *harmonic series* and is a very important object from calculus. We notice that each term in the sum is smaller than its predecessor, and the terms are getting arbitrarily small (so they are approaching 0).
3. This sum is important because despite the fact that the terms are shrinking to 0, the sum itself is *infinite*. When an infinite series does not sum to a number, we say that the series *diverges*.
4. The harmonic series diverges, which seems counterintuitive, so we ask our standard question, why?

B. A divergent sum.

1. A sneaky grouping of the terms in the harmonic series offers us some intuition about why the series sums to infinity (that is, diverges).
2. We first collect the numbers in groups of sizes that equal ever-higher powers of 2. That is, we group the series $1 + 1/2 + 1/3 + 1/4 + 1/5 + 1/6 + 1/7 + 1/8 + \cdots$ as: $1 + (1/2) + (1/3 + 1/4) + (1/5 + 1/6 + 1/7 + 1/8) + \cdots$.
3. We notice that this series is term-by-term larger than the series $1 + (1/2) + (1/4 + 1/4) + (1/8 + 1/8 + 1/8 + 1/8) + \cdots$.
4. This "smaller" series equals: $1 + 1/2 + 1/2 + 1/2 + \cdots$. Adding infinitely many halves together yields an infinite answer. Thus the "larger" harmonic series must be infinite as well.

C. Another argument showing the infinitude of the primes.

1. We now see why our argument to verify Euler's formula was "formal": The two expressions are indeed *not* numbers but *are* equal as mathematical expressions.
2. Using our new insight that the harmonic series diverges, we can apply Euler's product formula to give a modern proof that there are infinitely many prime numbers.
3. This proof is by contradiction: We will assume that there are only finitely many prime numbers and argue that this assumption leads to a contradiction—a logical fallacy.
4. If there were only finitely many prime numbers, then the product in Euler's formula, $(1/(1 - 1/2)) \times (1/(1 - 1/3)) \times (1/(1 - 1/5)) \times \cdots$, would have a last term. Thus we would have a product of a finite number of rational numbers (fractions), and that product would be another rational number.
5. However, by Euler's product formula we know that this product equals the harmonic series, which we just showed equals infinity. Therefore we are forced to conclude that there is a rational number (a ratio of two natural numbers) that equals infinity. This is impossible, and thus we have reached a contradiction.

6. This fallacy implies that our original assumption must have been false; hence, there must be infinitely many primes.
7. Notice how different this argument is from Euclid's original proof that there are infinitely many primes.

III. The likelihood that a number is "square free."

A. The likelihood of stumbling on an odd number.

1. Euler's general product formula has important implications into the study of primes.
2. To illustrate one implication, we consider a very simple question: What is the probability that a randomly selected natural number is odd?
3. We consider the *opposite* question: What is the probability that this number is even (i.e., a multiple of 2)? Since every other number is a multiple of 2, the probability of the number being even equals 1/2. To find the opposite probability, we compute $1 - 1/2 = 1/2$. So we conclude that the probability that the random number is odd is 1/2.
4. This elementary analysis can be extended to answer a much more interesting and subtle number question.

B. No repeated prime factors: What are the chances?

1. Moving beyond the prime numbers—those numbers that have just one number appearing in their prime factorization—we consider those numbers whose prime factorizations consist of no repeated primes. That is, those numbers for which the primes appearing in their prime factorizations appear only *once*.
2. These numbers are called "square free." For example, 6 is square free because no repeated primes appear in its prime factorization, 2×3. However 20 is *not* square free because it does have a repeated factor in its prime factorization, $2 \times 2 \times 5$. Similarly, 54 is not square free because $54 = 2 \times 3 \times 3 \times 3$.
3. If we were to pick a natural number at random, what is the probability that it is square free, that is, *not* a multiple of 2^2, 3^2, 5^2, 7^2, 11^2, and so forth, for each prime number?
4. Applying our thinking for the question of *not* being a multiple of 2, we see that the likelihood of *not* being a multiple of 2^2 equals $1 - 1/2^2$; the likelihood of *not* being a multiple of 3^2 equals $1 - 1/3^2$; and in general for any prime number p, the likelihood that a random number is *not* a multiple of p^2 equals $1 - 1/p^2$.
5. We will string all these probabilities together with multiplication as we would if we were flipping a coin again and again—that is, we will view the likelihood with respect to each prime as independent.
6. So the probability of having no prime appearing twice is: $(1 - 1/2^2) \times (1 - 1/3^2) \times (1 - 1/5^2) \times (1 - 1/7^2) \times \cdots$, which is the reciprocal of the product from Euler's general product formula. Therefore this product equals $1/(1 + 1/2^2 + 1/3^2 + 1/4^2 + 1/5^2 + 1/6^2 + 1/7^2 + \cdots)$, which can be written as $1/\zeta(2)$.

C. A very special sum.

1. Unlike the harmonic series, the terms from the infinite series $\zeta(2)$ do shrink to 0 fast enough so that the entire series does converge to a number.
2. This infinite series can be computed through some advanced mathematical ideas from calculus. The answer is $\zeta(2) = \pi^2/6$.
3. So the probability that a random natural number is square free is $1/\zeta(2) = 6/\pi^2 = 0.6079\ldots$, or about 61%.
4. Euler's product formula appears in unexpected places throughout mathematics and science.

Questions to Consider:

1. What is the probability that a natural number chosen at random is *not* a multiple of 7?
2. We have seen that the harmonic series $1 + 1/2 + 1/3 + 1/4 + 1/5 + \cdots$ diverges to infinity. How many consecutive terms do you need to add to get a partial sum that exceeds 2? How about 3?

Lecture Nine

The Prime Number Theorem and Riemann

Scope: In this lecture we close our explorations into analytic number theory by studying its crown jewel, the prime number theorem, which answers a question of great interest to mathematicians: Can we estimate how many primes there are up to a certain size? To improve the estimates within this important result we will return to Euler's general product formula and come upon one of the most important unsolved problems in all of mathematics—the Riemann Hypothesis. The truth of the Riemann Hypothesis would immediately imply a long list of deep results. While the issues surrounding the Riemann Hypothesis at first appear to be totally divorced from our "real world," we will mention some tantalizing new connections with physics through what are known as *random matrices*, which might hold the key to unlocking the mysteries of this long-standing open question about the atoms of the natural numbers—the primes. While a complex proof of the prime number theorem was found in 1896, many number theorists wondered if there was an "elementary" argument. Finally, in 1948 such a proof was found by two great mathematicians: Paul Erdös and Atle Selberg. This mathematical milestone led to one of the most famous disputes in number theory history. We will close this chapter of our course by describing some modern advances in the study of primes, some of which will allow us to return to the concept of arithmetic progressions. Finally we will ponder some famous questions involving prime numbers that remain mysteries to this very day.

Outline

I. The prime number theorem.
  A. How many primes are there?
    1. We close our study of the primes by returning to Euclid's theorem stating that there are infinitely many primes.
    2. Can we make this result more precise?

  B. A remarkable estimate.
    1. We write $\pi(n)$ to denote the number of primes less than or equal to n.
    2. So, for example, $\pi(25) = 9$ because there are nine primes that are less than or equal to 25: 2, 3, 5, 7, 11, 13, 17, 19, and 23.
    3. Euclid's theorem asserts that $\pi(n)$ approaches infinity as n gets larger and larger.
    4. Is there a formula for $\pi(n)$? This remains an open question seemingly impossible to answer.
  C. An "elementary" proof.
    1. By the late 18th century, French mathematician Adrien-Marie Legendre and the great Gauss noticed that the number of primes less than or equal to n, $\pi(n)$, seemed to be connected with the "natural logarithm" function, $\ln(n)$.
    2. The natural logarithm of a natural number n can be roughly viewed as approximately the number of digits n contains.
    3. Thus we see that $\ln(n)$ is a very slow-growing function.
    4. The conjecture was as n gets larger and larger, $\pi(n)$ gets closer and closer to $n/\ln(n)$.
    5. The great Russian mathematician Pafnuty Chebyshev proved in 1850 that *if* the quantity $\pi(n)/(n/\ln(n))$ approaches a number as n gets larger and larger, then that number must equal 1.
    6. In 1859 the great German mathematician Bernhard Riemann introduced a number of revolutionary ideas in his memoir *On the Number of Primes Less Than a Given Magnitude*. Among other things, he showed how this issue is connected with complex numbers (numbers involving the imaginary number $i = \sqrt{(-1)}$) and the zeta function, $\zeta(s)$, that we saw in Euler's general product formula. Today the zeta function is known as the *Riemann zeta function.*
    7. In 1896 French mathematician Jacques Salomon Hadamard and Belgian mathematician Charles de la Vallée-Poussin independently produced a proof of the prime number theorem: As n gets larger and larger, the number of primes up to n approaches $n/\ln(n)$. More precisely, as n gets larger and larger, the ratio $\pi(n)/(n/\ln(n))$ approaches 1.

II. The Riemann Hypothesis.
  A. The "error" in the prime number theorem.

1. The prime number theorem implies that as n gets larger and larger, $\pi(n)$ gets closer and closer to $n/\ln(n)$.
2. However for any particular n, $\pi(n)$ is not equal to $n/\ln(n)$; there is an error given by the difference between these two numbers.
3. How close are these two numbers in actuality for larger and larger values of n?

B. Bernhard Riemann and his famous hypothesis.

1. In Riemann's famous work, he found a profound connection between $\pi(n)$ and the zeta function: $\zeta(s) = 1 + 1/2^s + 1/3^s + 1/4^s + 1/5^s + 1/6^s + 1/7^s + \cdots$.
2. Riemann's insight was to extend the series $\zeta(s)$ to allow s to be a complex number, that is, $s = x + iy$, for real numbers x and y, and $i = \sqrt{(-1)}$.
3. Riemann studied the complex numbers s that were solutions to the following strange-looking equation: $\zeta(s) = 0$. Or, equivalently but even stranger: $1 + 1/2^s + 1/3^s + 1/4^s + 1/5^s + 1/6^s + 1/7^s + \cdots = 0$.
4. He proved that all the complex solutions $s = x + iy$ satisfy the condition that $0 \le x \le 1$ and showed that if these bounds could be tightened, then the error term in the prime number theorem could be reduced.
5. A key step in Hadamard's and de la Vallée-Poussin's proof of the prime number theorem was showing that all solutions satisfied $0 < x < 1$.
6. Riemann conjectured that *all* the solutions satisfied $x = 1/2$. This conjecture is now known as the *Riemann Hypothesis*.

C. What if it's true?

1. If the Riemann Hypothesis were true, then we would have a much smaller error term in the prime number theorem. In addition, we would learn an enormous amount about the prime numbers because there are literally hundreds of theorems that begin "Assuming the truth of the Riemann Hypothesis … ."
2. In 1900 the great German mathematician David Hilbert included the Riemann Hypothesis on his list of the 23 most important unsolved questions in mathematics. One hundred years later, the Clay Mathematics Institute in Cambridge, MA, listed it as one of its "Millennium Problems"—a correct and complete answer would result in a prize of $1 million.
3. It remains one of the most important open questions in all of mathematics.

D. Current state of knowledge.

1. There is a long list of partial results surrounding the Riemann Hypothesis.
2. From 2001 through 2005, a number theory program called "ZetaGrid" verified that the first 100 billion solutions to the equation had $x = 1/2$. Of course, this overwhelming data is not a general proof.
3. A new direction toward a possible proof of the Riemann Hypothesis is to study objects called *random matrices*. These are mathematical objects that were originally applied to better understand the quantum behavior of larger atoms in physics.

III. The drama behind an "elementary" proof of the prime number theorem.

A. A search for an "elementary" proof.

1. The original proof of the prime number theorem was extremely clever and subtle (especially in demonstrating that $x < 1$ for all the "zeros" of the Riemann zeta function).
2. In 1921 the great British analytic number theorist G. H. Hardy wondered if an "elementary" proof of the prime number theorem could be found—that is, a proof that involved only very simple properties of functions but in an extraordinarily ingenious manner.
3. Many believed that such an "elementary" proof might not be possible.

B. Paul Erdös, Atle Selberg, and their contributions.

1. In 1948 Paul Erdös announced that he and Atle Selberg had found a truly "elementary" proof that involved only basic properties of the logarithm.
2. This announcement stunned the mathematical world.
3. Paul Erdös was a Hungarian mathematician who published well over 1500 mathematical articles with over 500 coauthors from around the world. He was also a nomad, having no true academic affiliation for most of his life.

4. His prolific and foundational work inspired and fed new branches of mathematics including *graph theory*, *combinatorial number theory*, and *elementary number theory*.
5. Atle Selberg was a Norwegian mathematician who spent much of his career at the Institute of Advanced Study at Princeton.
6. He produced profound results in advanced areas of number theory including automorphic forms, and he introduced several new areas of study including the "Selberg sieve" and the "Selberg trace formula."

C. Their important proof.

1. Their "elementary" proof of the prime number theorem was so sensational that in 1950 Selberg was awarded the Fields Medal (the mathematical equivalent of the Nobel Prize).
2. In 1952 Erdös received the Cole Prize (one of the most prestigious prizes in mathematics).

D. The controversy that ensued.

1. A serious controversy arose over who should receive credit for what part of the proof.
2. In March 1948, Selberg discovered an important formula involving primes but did not publish it.
3. Several months later, Selberg shared with Hungarian mathematician Paul Turan an inequality he discovered (now known as the *fundamental formula*). Without Selberg's objection, Turan gave a lecture outlining Selberg's recent work.
4. Erdös, who was in the audience, quickly exclaimed, I think you can also derive $\lim p_{n+1}/p_n = 1$ (as n approaches infinity) from this inequality.
5. Within a few hours Erdös produced an ingenious proof of his extremely important assertion. A day later, when Erdös shared this news with Selberg, Selberg responded with, You must have made a mistake.
6. A few days later, Selberg, using his formula involving logarithms and primes together with Erdös's important result, was able to devise an "elementary" proof of the prime number theorem. The key ingredient, however, was Erdös's theorem.

7. Erdös suggested that the two collaborate and write a joint paper, but Selberg suggested that each write their own papers based on their own work. Erdös found this objectionable.
8. To make matters worse, news started to spread about this amazing breakthrough, but the rumor attributed the result to Erdös. In the fall of 1948, someone greeted Selberg with, Have you heard the exciting news of what Erdös has proven? This did not help the situation.
9. The two did publish their papers separately, including mention of each other's work. However, the two did not speak to each other again for 45 years.

IV. Further advances on the distribution of the primes.

A. Dirichlet's theorem on primes in arithmetic progressions.

1. We recall the idea of an arithmetic progression: We start with a number and continue to add a fixed amount. For example, start with 1 and repeatedly add 17 to obtain 1, 18, 35, 52, and so forth.
2. Gauss wondered if such arithmetic progressions always contained prime numbers. In this example we have 1, 18, 35, 52, 69, 86, 103, … , and 103 is the first prime number we found.
3. In 1837, German mathematician Johann Dirichlet proved that given any natural numbers A and B not sharing any prime factors, the arithmetic progression A, A + B, A + 2B, A + 3B, A + 4B, and so on, will always contain infinitely many prime numbers. This extends Euclid's theorem on the infinitude of primes.

B. Arithmetic progressions of primes.

1. Suppose we list all the prime numbers in order: 2, 3, 5, 7, 11, 13, 17, 19, … .
2. Within this list, do we see any pieces that form an arithmetic progression? For example, 3, 5, 7 forms an arithmetic progression (we repeatedly add 2). What is the *longest* arithmetic progression found in the list of primes?
3. In 2004 some groundbreaking work was done in this direction by Ben Green and Terence Tao. They proved the astounding result that there are arbitrarily long arithmetic progressions within the list of prime numbers.

V. Famous open questions involving prime numbers.

A. Twin primes. Are there infinitely many pairs of primes that differ by 2? For example, (3, 5), (5, 7), (11, 13). These pairs are known as *twin primes*. Notice that (13, 17) is not a pair of twin primes because their difference is not 2: $17 - 13 = 4$. The Twin Prime Conjecture states that there are infinitely many twin primes. But a proof continues to elude us.

B. Goldbach's conjecture.

1. We notice that $6 = 3 + 3$ (the sum of two primes); $8 = 3 + 5$; $10 = 5 + 5$; $12 = 5 + 7$; $14 = 7 + 7$; and $16 = 5 + 11$. Here we see that each of these even numbers can be expressed as the sum of two primes.
2. The Goldbach conjecture states that every even number greater than 2 can be written as the sum of two prime numbers.
3. The conjecture was first made by Christian Goldbach in a letter to Euler dated June 7, 1742.
4. Even though the conjecture has been shown to hold for all even numbers up to 3×10^{17}, a proof that it holds for *all* even numbers has yet to be found.

C. Skewes number.

1. We have seen that $\pi(n)$ approaches the function $n/(\ln(n))$. However, there is another function that behaves like $n/(\ln(n))$ and also approximates $\pi(n)$. This is called the *logarithmic integral* and is written $\mathrm{Li}(n)$. It has been shown that $\pi(n) - \mathrm{Li}(n)$ approaches 0 as n gets larger and larger.
2. In 1914 British mathematician John Littlewood proved that the quantity $\pi(n) - \mathrm{Li}(n)$ changes from positive to negative infinitely many times.
3. However, for all values up to around 10^{22}, the quantity has been negative (that is, $\mathrm{Li}(n)$ has been larger than $\pi(n)$). Given Littlewood's result, we know that $\mathrm{Li}(n)$ must at some point be smaller than $\pi(n)$. But when?
4. South African mathematician Samuel Skewes in 1933 proved that, assuming the truth of the Riemann Hypothesis, $\mathrm{Li}(n)$ must be smaller than $\pi(n)$ for some n less than $10^{10^{10^{34}}}$. Now known as *Skewes number*, it was described by G. H. Hardy as, "the largest number which has ever served any definite purpose in mathematics."

Questions to Consider:

1 Can there be an arithmetic progression of three consecutive prime numbers with increments equal to 3; that is, can there exist three numbers n, $n + 3$, and $n + 6$ for which each number is prime?

2. A Fermat number is a number of the form $2^{2^n} + 1$. Find two values for n that make the corresponding Fermat numbers equal to primes.

Lecture Ten

Division Algorithm and Modular Arithmetic

Scope: Divisibility is one of the central pillars of number theory. A number evenly divides into another if the first number is a factor of the second. In fact, our work on factorization and the primes from our sojourn into analytic number theory underscores the importance of divisibility. If a number does *not* evenly divide into another, then there is a nonzero remainder resulting from that division. Here we will study these remainders and discover a new and delicate arithmetic known as *modular arithmetic*. We will begin by revisiting the "long division" we saw in elementary school and its sophisticated number theory counterpart known as the *division algorithm*. By repeated applications of the division algorithm we come upon a method for finding the greatest common divisor of any two natural numbers. This important process is known as the *Euclidean algorithm*. We will introduce the main ideas behind modular arithmetic and make the realization that it simply captures the mathematics of cycles—such as hours in the day, in which we return to the same time every 24 hours, or days in the week, in which we return to the same day every seven days. The study of the arithmetic of remainders is important from a mathematical standpoint and also from a practical one. As an illustration, we will consider the sequence of numbers at the bottom of every bank check, called the bank routing number. We will discover a number theoretic coding scheme that involves the modular arithmetic of remainders. Similar error-checking schemes underlie the zebra-striped bar code known as the Universal Product Code (UPC) that is tattooed on nearly all merchandise.

Outline

I. Long division and the division algorithm.
  A. A return to long division from long ago.
    1. To understand the personality of a natural number n, we have been studying the prime numbers that evenly divide into n. We now focus more generally on the idea of division.
    2. Using long division, we can divide 47 by 3 and get the answer (the quotient) of 15 with a remainder of 2.
  B. A focus on remainders.
    1. Suppose we wish to divide 51 by 4. Before we begin, we wonder, what are the possible values for the remainder?
    2. In this example, because we are dividing by 4, the possible remainders are 0, 1, 2, and 3.
    3. Four goes into 51 twelve times, and we are left with a remainder of 3. If we divide a number a by b, then the remainder will be a number from $0, 1, 2, \ldots, b - 1$.
    4. The remainder equals 0 if and only if b divides evenly into a—that is, when b is a factor of a.
  C. The division algorithm.
    1. The formalization of long division is called the *division algorithm*: For natural numbers a and b, if we divide a by b, then there exists a unique quotient q and remainder r satisfying $a = bq + r$ and for which $0 \leq r < b$.
    2. In our previous examples we would write: $47 = 3 \times 15 + 2$ and $51 = 4 \times 12 + 3$. Thus without any further work we conclude that 3 is not a factor of 47 and 4 is not a factor of 51.

II. Repeated division and the Euclidean algorithm.
  A. The greatest common divisor.
    1. We now move from the study of the arithmetic personality of a natural number (through factorization into primes) to seeing similarities between the arithmetic personalities of two natural numbers.
    2. Given two numbers, we wish to find the largest number that is a common factor of the two given numbers.
    3. For example, if both numbers are even, then we know they both share the common factor of 2, but perhaps they have even more factors in common.
    4. The largest number that is a common factor to both a and b is called the *greatest common factor* of a and b. This number is also known as the *greatest common divisor* of a and b.
    5. If the two given numbers are small, we can easily find their greatest common factor by factoring each number into primes and picking out all the common factors. For example, if we wish to find the greatest common factor of 30 and 42, we can

just factor each: $30 = 2 \times 3 \times 5$, and $42 = 2 \times 3 \times 7$, and then multiply all the common factors: $2 \times 3 = 6$. Thus 6 is the greatest common factor of 30 and 42.

6. This "divide and conquer" method will always work in theory but is impractical for large numbers.

B. The Euclidean algorithm.

1. For large numbers, the question remains, Is there an easy way to find the greatest common divisor of two numbers? The answer is yes: We convert a very difficult task into many easy tasks.
2. In his *Elements of Geometry*, Euclid describes an algorithm for finding the greatest common divisor of two numbers. This algorithm is perhaps the oldest one ever devised and is now known as the *Euclidean algorithm.*
3. The algorithm is based on an important fact: Whenever we know that $a = bq + r$, then the greatest common factor of a and b equals the greatest common factor of b and r. We can repeatedly apply the division algorithm to "divide and conquer" our way to the greatest common factor of two numbers.

C. Some illuminating illustrations.

1. To illustrate the idea, we apply the Euclidean algorithm to find the greatest common factor of 30 and 42.
2. By the division algorithm we see that $42 = 30 \times 1 + 12$. So the greatest common factor of 42 and 30 is the same as for 30 and 12 (these are smaller numbers). We now apply the division algorithm with 30 and 12: $30 = 12 \times 2 + 6$. Again we have that the greatest common factor of 30 and 12 is the same as the greatest common factor of 12 and 6.
3. Now we can see that the greatest common factor of 12 and 6 is 6. We can see this because 6 is a factor of 12, that is, $12 = 6 \times 2 + 0$. When this repeated division algorithm process generates a remainder of 0, then the *previous* remainder (in this example, 6) is the greatest common factor of the original two numbers. This process is the *Euclidean algorithm.*

4. If we apply the Euclidean algorithm to find the greatest common factor of 217 and 245, then we repeat the division algorithm as we just outlined:

$$245 = 217 \times 1 + 28$$
$$217 = 28 \times 7 + 21$$
$$28 = 21 \times 1 + 7$$
$$21 = 7 \times 3 + 0.$$

5. Once we find a remainder of 0, we find the previous (nonzero) remainder, and that equals the greatest common factor. Thus we see that the greatest common factor of 217 and 245 is 7 (and we can check that $217 = 7 \times 31$ and $245 = 5 \times 7 \times 7$).

D. Relatively prime numbers.

1. Recall that a natural number greater than 1 is prime if it has no factors other than 1 and itself. We now extend this notion to pairs of numbers.
2. We say two natural numbers a and b are *relatively prime* if they have no prime factors in common—that is, if their greatest common factor is 1.
3. For example, 6 and 49 are relatively prime (notice that $6 = 2 \times 3$ and $49 = 7 \times 7$). On the other hand, 12 and 20 are *not* relatively prime because they share the common factor of 4.
4. If we use the Euclidean algorithm with a and b, then those two numbers are relatively prime if and only if the last nonzero remainder equals 1. For example: $49 = 6 \times 8 + 1$.
5. If we backward-solve for the remainder of 1, we find that $49 - 6 \times 8 = 1$, and then we see we can always find natural numbers x and y that are solutions to $49x - 6y = 1$ (in this case, $x = 1$ and $y = 8$). In general, if two given numbers a and b are relatively prime, then we can find natural numbers x and y that are solutions to $ax - by = 1$. This little fact will be extremely useful in our discussion of cryptography in Lecture Twelve.

III. Modular arithmetic of remainders.

A. A world of cycles.

1. Given two natural numbers, if the division algorithm gives a remainder of 0, then we know that one number divides the

other; if the remainder is 1, then we know that the two numbers are relatively prime.

2. We now focus on the remainders we see after we divide. As an illustration, let's consider just the remainders when the numbers 0, 1, 2, 3, 4, 5, 6, and so forth are divided by 4.
   Numbers: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, ...
   Remainder (÷ 4): 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, 2, ...
3. We observe that the remainders cycle through the numbers 0, 1, 2, and 3.

B. The cycles of clock arithmetic.

1. We can view this cycle as similar to that of a clock. In the previous example, once we arrive at 3, the next number we see brings us back to 0.
2. This is the same arithmetic as we use to tell time (not only in terms of seconds, minutes, and hours, but also in days of the week and months in the year). For example, on a 12-hour clock, fourteen o'clock is really 14 − 12, which is two o'clock—we cycle around.
3. The arithmetic of remainders is known as *modular arithmetic*.
4. Modular arithmetic corresponds to the arithmetic of cycles we use for time. For example, suppose we are considering division by 4. If a number with a remainder of 1 is added to a number with a remainder of 1, then the sum will have a remainder of 2 (for example, 5 + 9 = 14, and the remainder when 14 is divided by 4 is 2).
5. If we again consider division by 4, then when a number with a remainder of 2 is added to a number with a remainder of 3, the sum will have a remainder of 1 since we cycle 2 + 3 = (2 + 1 + 1) + 1 = 0 + 1 = 1 (as remainders when dividing by 4). (For example, 6 + 11 = 17, and the remainder when 17 is divided by 4 is 1). We only need to focus on the cycles of the remainders and not the quotients. Thus we are always working with numbers relatively small to the divisor.
6. We refer to this arithmetic of remainders when dividing by 4 as arithmetic "modulo 4" or "mod 4." So we would say 6 + 11 ≡ 1 (mod 4). The symbol ≡ is read "congruent" and means "equal remainders" when divided (in this case) by 4.

C. A deeper understanding of numbers.

1. Although people have been studying remainders since at least the 3rd century, when the Chinese were proving interesting theorems involving the cycles of remainders, modular arithmetic was formally introduced by Gauss in 1801.
2. Modular arithmetic is a powerful tool that allows us to establish subtle divisibility results through the use of basic arithmetic. For example, if the difference of two numbers is congruent to 0 (mod m), then that tells us that those two numbers will have the *same* remainders when each is divided by m, without the need to perform the long division.
3. As an illustration, again we consider arithmetic mod 4 (remainders when we divide by 4). Notice that 103 − 95 = 8 ≡ 0 (mod 4). So 103 will have the same remainder as 95 when divided by 4 *without ever performing the long division*! We can check that 103 = 4 × 25 + 3 and 95 = 4 × 23 + 3 and see that both have remainders equal to 3.

IV. Applications of modular arithmetic.

A. Breaking into the bank routing numbers.

1. The bank routing number is the nine-digit number located on the lower left corner of any check. It identifies the bank from which the check is issued.
2. Computers scan the routing number (along with the bank account number that appears to the right of the routing number) and electronically make the appropriate withdrawal. To prevent errors in reading these numbers, encoded in the routing numbers is a check that involves modular arithmetic.
3. To check a bank routing number, we take the nine digits, say A, B, C, D, E, F, G, H, I, and produce the following (strange) number: 7A + 3B + 9C + 7D + 3E + 9F + 7G + 3H + 9I. We now consider this auxiliary number modulo 10 (that is, consider its remainder when divided by 10). The remainder should be 0, so if the remainder is *not* 0, we know we have an error.
4. Divisibility by 10 is very easy to check: A number is evenly divisible by 10 (so has remainder 0) if and only if the number ends in a 0.

5. For example, one branch of Citizens Bank has a routing number 036 076 150. If we produce the corresponding auxiliary number: $7 \times 0 + 3 \times 3 + 9 \times 6 + 7 \times 0 + 3 \times 7 + 9 \times 6 + 7 \times 1 + 3 \times 5 + 9 \times 0 = 160$, it has a remainder of 0 when divided by 10 ($160 \equiv 0 \pmod{10}$), which is consistent with a valid routing number.
6. We can also use this code to determine a missing digit in a bank routing number. For example, suppose we were able to only partially read a Williamstown Savings Bank routing number. Suppose we only read 211 872 94[] (here the last digit is blocked from sight).
7. We compute the auxiliary number for this bank as best we can: $7 \times 2 + 3 \times 1 + 9 \times 1 + 7 \times 8 + 3 \times 7 + 9 \times 2 + 7 \times 9 + 3 \times 4 + 9 \times []$, which simplifies to $196 + 9 \times []$. We know this number must have a 0 remainder when divided by 10. To have a remainder of 0 (mod 10), we must find a multiple of 9 that ends in a 4. So we need to determine what digit [] when multiplied by 9 will end in a 4. The answer is 6. If we let [] equal 6, then our auxiliary number becomes 196 + 54, which equals 250, giving us a remainder of 0 when divided by 10 and confirming the last digit of the bank code.
8. This error-detection method is guaranteed to detect most common errors: interchanged digits or a single digit read incorrectly.

B. Similar coding schemes and modular arithmetic.
1. Similar coding schemes using modular arithmetic and remainders are used to check Universal Product Codes (UPCs), ISBNs on books, and even driver's licenses in certain states.
2. We employ modular arithmetic—the mathematics of cycles—every day, both consciously when we make appointments or look at a clock and also unconsciously behind the scenes in our technological world.
3. Number theory allows us to see and understand those invisible instances with great clarity.

Questions to Consider:

1. We are told that the difference between the numbers 123,456,789 and 213 has a factor of 123. Using this fact, determine the remainder when 123,456,789 is divided by 123.
2. Examine one of your personal checks. Find the bank routing number in the lower left corner and check that it satisfies the formula described in the lecture.

Lecture Eleven

Cryptography and Fermat's Little Theorem

Scope: In this lecture we will combine ideas from the theory of prime numbers and modular arithmetic to develop an extremely powerful, important, and counterintuitive application: public key cryptography. We will open with a brief historical overview of ciphers and the need for encrypting messages. We then will consider the seeming ridiculous question, Is there an encryption method in which everyone can publicly announce the encryption scheme to code messages yet only the receiver can decode the messages? The surprising answer is that such a public key encryption scheme does indeed exist, and it offers a currently unbreakable coding method. In fact, we use this encryption scheme every day. The main theorem behind this modern method is a 350-year-old result due to Pierre de Fermat involving primes and modular arithmetic. The mathematical secret exploited in this coding method is the reality that factoring large natural numbers into primes is, in practice, extremely difficult, if not "impossible."

Outline

I. A brief history of secret ciphers.

A. A need for sharing secrets.

1. Throughout history, humankind has had a desire to keep certain information hidden from certain individuals.

2. Communications involving business transactions, national security, military plans, and even some romantic trysts needed to be kept secret from various parties.

B. Early ciphers.

1. The earliest known example of cryptography was found in Egyptian hieroglyphics around 2500 B.C.E. These may have been for amusement rather than secret communication.

2. The earliest simple substitution ciphers, known as *monoalphabetic substitution ciphers*, may have been those used by Hebrew scholars around 550 B.C.E.

3. A *Caesar cipher*, named after Julius Caesar, is a special case of a monoalphabetic substitution cipher in which each letter is replaced by the letter a fixed number of positions down the alphabet. Such monoalphabetic encryption schemes are very easy to break.

4. Cryptography was known in India by the 1st century C.E., during the time of the famous *Kama Sutra*, in which encryption was suggested as a method for secret communication between lovers.

C. Machines that encode and decode.

1. Ancient Greeks used transposition ciphers, in which elements of the text are rearranged according to a particular scheme. They used a tool called a *scytale* to encrypt and decrypt messages.

2. The Jefferson disk, invented by Thomas Jefferson in 1795, was an encryption and decryption device involving circular disks. A variation of the Jefferson disk was used by the United States Army from 1923 through 1942.

3. The idea of using disks and cogs led to one of the most famous encryption devices, known as the *Wehrmacht Enigma*, which was used by the Nazi military before and during World War II. The Enigma was so complex that for some models, the number of possible rotor configurations exceeded 10^{22}. The great British mathematician and computer scientist Alan Turing was a key figure in cracking the Enigma.

D. Breaking codes.

1. Long before Turing and his team broke the Enigma in the 1940s, people were breaking codes.

2. The first systematic work in cryptanalysis may have arisen from an in-depth religious analysis of the Koran around 800 C.E. Arabs developed the method of frequency analysis to break codes.

3. Very effective for monoalphabetic ciphers, the frequency analysis represents what may be the earliest recorded work in probability and statistics.

4. Frequency analysis can be applied in the recreational solving of cryptoquote puzzles in newspapers.

II. Should and must we trust our allies?

A. A fundamental flaw.

1. In all these coding schemes, there is a basic reality: We must trust our friends.
2. Friends know the encryption and decryption methods for sharing confidential information.
3. Our friends might be totally trustworthy, but if they accidentally lose the coding instructions, then the encryption system's security would be breached.

B. Reversing the encryption process.

1. In the ciphers we described, to decode an encrypted message, one reverses the encryption process.
2. Thus if people know how to encode a message to us, then they can also decode messages.

III. An intuitive look at a public secret code.

A. A cipher fantasy.

1. In the best of all possible worlds, we would not have to trust our friends.
2. If they lose the codebook, it would not jeopardize the coding scheme.

B. Making encoding both public and private.

1. Ideally, knowing how to encode a message would not provide any information as to how to decode the message.
2. If this fantasy were real, then there would be no need to keep the encoding process a guarded secret.
3. Instructions on how to encode could be made public, and only the decoding process would need to be kept secret.
4. In fact, in this fantasy, the encoded messages could be made public as well.
5. Because the public encoding process could be run backwards to decode the message, there is a need for a secret within the public encryption process.

C. An intuitive insight through number theory.

1. Here we apply the concepts we have seen so far to show that such a cryptography fantasy can be made a reality.
2. The main question remains: How can the encryption scheme be at once public (everyone knows how to code messages) and private (only the rightful receiver can decode the messages)?
3. Such ciphers are known as *public key codes*.

4. Combining the concepts of prime numbers together with modular arithmetic in a clever way allows us to make our fantasy a reality.

D. Shuffling messages.

1. We first offer a metaphor that captures the idea of this modern encryption scheme.
2. Suppose we take a brand new deck of 52 playing cards and perform eight perfect shuffles (also known as *faro shuffles*). Then we would have the cards returning to their original order.
3. If we performed five perfect shuffles, then the order of the cards would look thoroughly mixed, without any semblance of pattern or structure. However, we know a systematic method that would return this jumbled mess back into a familiar, less chaotic pattern. We perform three more perfect shuffles and *voilà*—the cards are transformed from a random mess to their original order!
4. We could employ this shuffling idea to produce an encryption scheme. Our friend could write a message to us, one letter on each card, and encode the message by performing n perfect shuffles (a pre-agreed upon number, n).
5. We would receive the shuffled deck and know exactly what to do: We would perform $8 - n$ perfect shuffles to decode the message.
6. To have this scheme truly fulfill our encryption fantasy, we need to figure out how to mathematically "shuffle" our message and then how to make the shuffling process public.
7. The public feature arises from the fact that factoring extremely large natural numbers is *practically* impossible despite the reality that we know that such a factorization is possible *in theory*.

IV. Shuffling numbers with Fermat's Little Theorem.

A. Pierre de Fermat: the man and his mathematics.

1. Pierre de Fermat was a 17^{th}-century French lawyer who explored number theory as a leisure activity. He rarely published his scholarly work.
2. His body of work comes only from his notes and correspondence with mathematicians. He would provide few

if any details into the proofs of his assertions. There were and remain mathematicians (including Gauss) who doubt Fermat had complete proofs of all his mathematical assertions. Many of his claims were not proved until 100 years after he died.

3. One assertion of his was very stubborn; no one was able to prove or disprove it. Since it was the last assertion that remained unverified, it became known as *Fermat's Last Theorem*. We will study this famous question and the solution that was over 350 years in the making in Lectures Fourteen and Eighteen.
4. Fermat produced an extremely important and useful theorem that holds the key to our cryptography conundrum. To distinguish this result from his "Last Theorem," this result is known as *Fermat's Little Theorem*.

B. A pattern within the primes.

1. To explore Fermat's Little Theorem, we will consider all the possible nonzero remainders when dividing by 5. Those remainders are 1, 2, 3, and 4.
2. We now consider the remainders when we first multiply these four numbers by 2 and divide by 5, and then we repeat the process with the new list. We would see:

	1, 2, 3, 4
× 2:	2, 4, 6, 8
mod 5:	2, 4, 1, 3
× 2:	4, 8, 2, 6
mod 5:	4, 3, 2, 1
× 2:	8, 6, 4, 2
mod 5:	3, 1, 4, 2
× 2:	6, 2, 8, 4
mod 5:	1, 2, 3, 4

3. If we now just focus on the remainders, we first see 1, 2, 3, 4, and then 2, 4, 1, 3, then 4, 3, 2, 1, then 3, 1, 4, 2, and finally 1, 2, 3, 4. Notice this process just shuffles the numbers 1, 2, 3, 4, and we end back where we started.
4. Thus if we focus just on the numbers in the second location, we see 2 then 4 then 3 then 1, then back to 2. That implies that $2 \times 2 \times 2 \times 2$ must have a remainder of 1 when divided by 5.

C. Fermat's Little Theorem.

1. Fermat generalized this last observation. Fermat's Little Theorem: Given a prime number p and any natural number a that is relatively prime to p, then when we divide a^{p-1} by p, the remainder equals 1. Phrased using the congruence notation, we would say $a^{p-1} \equiv 1 \pmod{p}$.
2. As a further illustration, still with the prime $p = 5$, we consider the number 3 and compute $3^4 = 81$, which indeed has a remainder of 1 when divided by 5.
3. In fact, without any calculation at all, we know the remainder when 5 is divided into 777^4. By Fermat's Little Theorem, the remainder equals 1!
4. Moreover, the remainder when 29 is divided into $1{,}000{,}000^{28}$ equals 1!

D. Applications of an ancient theorem.

1. Fermat first stated this result in a letter dated October 18, 1640. He did not include a proof. Instead he wrote, "I would send you the demonstration, if I did not fear it being too long." The first published complete proof is due to Euler from 1736.
2. In the next lecture we will apply this old theorem about primes to the modern technological world of communication.

Questions to Consider:

1. What are some of the important uses of encryption in our day-to-day lives?
2. Without performing any calculations at all, find the remainder of 29 raised to the 30th power, divided by 31.

Lecture Twelve

The RSA Encryption Scheme

Scope: We open this lecture by celebrating the theorem, more than 350 years old, known as *Fermat's Little Theorem*, which connects the primes with modular arithmetic and whose utility permeates throughout all of number theory. It is this important number theoretic result that represents the key to unlocking public key cryptography. Here we will introduce and describe the popular RSA encryption scheme. This clever method of creating ciphers is not only the actual encryption scheme used millions of times a day but also holds within it some deep mathematical ideas. This modern reality of encryption brings to light a number of weighty issues, including the value of information, electronic signatures, and the possibility or impossibility of breaking such a code. As we will see, these questions highlight the interplay between the practical world of our modern technological times and the purely abstract, timeless theorems of number theory. The next time we enter our credit card number on an Internet site or use an ATM, we will realize that we are in fact employing some classical theorems from the theory of numbers in a clever and novel manner.

Outline

I. The return of the primes and Fermat's Little Theorem.

A. Fermat's Little Theorem.

1. We recall Fermat's Little Theorem: Given a prime number p and any natural number a that is relatively prime to p, then when we divide a^{p-1} by p, the remainder equals 1. (Phrased using the congruence notation, we say $a^{p-1} \equiv 1 \pmod{p}$).

2. To see the power of this result, suppose we are given the prime number 7919 (and told that it is prime!). Then for any natural number n that is smaller than 7919, we know that the remainder when n^{7918} is divided by 7919 equals 1. For example, if 5862^{7918} were to be divided by 7919, we know the remainder: 1. No actual multiplication or division is required!

B. The big ideas behind the "little" theorem.

1. Let p be a prime number. Then where did that $p - 1$ exponent come from?

2. Recall from the last lecture we considered all the possible nonzero remainders when a number is divided by p. Those remainders are $1, 2, 3, \ldots, p - 1$.

3. How many of these numbers are relatively prime (share no common factors larger than 1) to p? Again, since p is a prime and the remainders are all less than p, we quickly see that each of them is relatively prime to p. Therefore there are $p - 1$ remainders that are relatively prime to p.

4. The fact that there are $p - 1$ remainders all relatively prime to p is the mathematical key to establishing Fermat's Little Theorem in general. The proof of this theorem, which we will not consider here, incorporates generalized notions from the algebra we have learned in school—an advanced area of mathematics known as *abstract algebra*.

C. Euler's extension of Fermat's result.

1. Even though we will not give the complete proof of Fermat's Little Theorem, we can apply the reasoning we just offered for why the exponent in the theorem is $p - 1$ to discover a generalization of Fermat's result.

2. In particular, is there a corresponding theorem in the case in which we divide by a composite number (rather than the prime p)?

3. The answer is yes, and this extension of Fermat's Little Theorem was discovered by Euler. Let n be any natural number (prime or composite). We now consider all the possible nonzero remainders after division by n: $1, 2, 3, \ldots, n - 1$.

4. Next we count how many of those remainders are relatively prime to n. Recall that in the case in which n is prime, all the remainders are relatively prime to n. Let us write r for the number of remainders that are relatively prime to n.

5. Given the above, Euler proved that for any natural number a that is relatively prime to n, the remainder when a^r is divided by n equals 1. Symbolically, we say: $a^r \equiv 1 \pmod{n}$.

6. This result is known as *Euler's Theorem*. We notice how this result coincides with Fermat's Little Theorem in the case in which n is a prime number.
7. As an example, if we want to apply Euler's Theorem with a divisor of 21, then we must find out how many of the nonzero remainders from 1, 2, ... , 20 are relatively prime to 21. There are 12 such numbers. Therefore for any number a relatively prime to 21, the remainder when a^{12} is divided by 21 equals 1. For example, $(10^{12})^{12} \equiv 1 \pmod{21}$.

II. An introduction into the RSA encryption scheme.

A. Revealing the "R," "S," and "A" behind RSA.

1. In 1977, Ron Rivest, Adi Shamir, and Leonard Adleman, all at MIT, announced an encryption scheme involving primes and modular arithmetic. This encryption scheme is now known as "RSA" in honor of these three mathematicians.
2. A few years earlier, in 1973, British mathematician Clifford Cook created a similar encryption scheme. However, Cook was working for British intelligence, and thus his work remained unknown until it was declassified in 1997. Cook's work was more of theoretic interest rather than a practical cipher since the calculations required exceeded the capacities of computers in the early 1970s.

B. Setting up an RSA public key code.

1. We introduce the steps involved in the RSA encryption scheme with an illustration involving small numbers.
2. First we need to set up the means by which people can encode messages to us. We select two different prime numbers. Here we chose the tiny primes 3 and 7. We multiply them together and find 21.
3. Next we consider the product of 1 less than each of these two primes: $(3 - 1) \times (7 - 1) = 2 \times 6 = 12$.
4. We now select any natural number that is relatively prime to 12; here we pick 29. From our discussion on the Euclidean algorithm in Lecture Ten, we recall that because 29 and 12 are relatively prime, we can find natural numbers x and y that satisfy the equation $29x - 12y = 1$. In this example, we can let $x = 5$ and $y = 12$. So $(29 \times 5) - (12 \times 12) = 145 - 144 = 1$.

5. We announce the numbers 29 and 21 to the entire world (they are the numbers used for encrypting messages to us); we keep the number 5 a secret—we do not reveal this number to *anyone*, even our friends and allies. We destroy all the other numbers.

C. Encoding and sending secret messages.

1. Suppose now that someone wishes to send us a message letting us know that she will be arriving on the "J" train. She first looks up our encryption numbers and, in this simple example, finds 29 and 21. In actuality these numbers would be enormous.
2. She then translates the message "J" into a natural number using the conversion A = 01, B = 02, ... , Z = 26. So we see that J = 10. She is now ready to encode the message "10" to us.
3. To encrypt the number 10, she computes the remainder when 10^{29} is divided by 21 (notice that 29 and 21 are the two numbers we made public to be used in this manner for encryption).
4. It is easy for computers to find this remainder, which in this example equals 19. The number 19 is the encoded version of "J." She then sends us the secret message 19, which she can post where everyone can see it.

D. Receiving and decoding messages.

1. We receive the encoded message "19," and now have to decode it. To do so, we use the public number 21 and the secret number 5 that *no one* knows.
2. We find the remainder when 19^5 is divided by 21. The remainder equals 10, the original message, which we convert to the letter J. We just decoded the message.

E. Why did this decoding process work?

1. To see why this decoding scheme genuinely works without performing any calculations, we consider the encoded and decoded numbers before we divide by 21.
2. The original message was 10. To encode it, our friend considered 10^{29} (the remainder when divided by 21 is the encrypted message). If we now take this number and raise it to our decoding exponent, 5, we would see: $(10^{29})^5 = 10^{29 \times 5}$.

3. We now recall that these numbers were selected so that: $(29 \times 5) - (12 \times 12) = 1$; that is, $29 \times 5 = 1 + (12 \times 12)$. Applying this equality we see: $(10^{29})^5 = 10^{29 \times 5} = 10^{1+12 \times 12} = 10 \times 10^{12 \times 12} = 10 \times (10^{12})^{12}$. The remainder when 10 is divided by 21 is equal to 10. By Euler's Theorem, as we have already seen, the remainder when $(10^{12})^{12}$ is divided by 21 equals 1. So the remainder when the product $10 \times (10^{12})^{12}$ is divided by 21 equals 10×1, which equals 10: the original message!
4. In actual practice, instead of starting with small primes such as 3 and 7 and taking their product to get 21, the two primes used are enormous, and thus their product is larger still—a number so large that factoring it is, for all practical purposes, impossible.

III. RSA in general.

A. Setting up an encryption key.

1. To set up an RSA encryption scheme, we first select two (large) different primes p and q. Let us define $m = p \times q$ and $k = (p - 1) \times (q - 1)$. (In our simple example, $p = 3$ and $q = 7$; $m = 21$; and $k = 12$.)
2. Next we select any (large) natural number that is relatively prime to k; let us call this large natural number e. (So in our example, $e = 29$.)
3. We now find natural numbers x and y that satisfy $ex - ky = 1$. (In our example, $x = 5$ and $y = 12$.)
4. We publicly announce the encryption scheme to send us messages: the numbers e and m. The number m, in practice, is so large that no one can factor it.
5. We keep x a secret from everyone and then destroy all other numbers. We are now ready to receive encrypted messages.

B. Encrypting messages.

1. Suppose now that our friend wishes to send us a message. She first converts it to a number, let us call it W, that is relatively prime to m and also less than m.
2. She then computes the remainder when W^e is divided by m. Let us call this remainder C. The number C is the encrypted version of W. She sends us the encrypted message "C."

C. Decrypting messages. If we receive the encrypted message "C," we know to compute the remainder when C^x is divided by m. That remainder will always equal the original W; that is, we have just decrypted the coded message.

D. Does the decoding scheme always work?

1. It is a theorem that this scheme of decoding will always return the original message, "W."
2. The proof of this theorem follows the identical steps we used to see why the decoding scheme worked in the specific example we considered.
3. This RSA scheme and related schemes are the most popular methods of encryption used today in banking, Internet commerce, and secure communication.

IV. Electronic signatures and the value of information.

A. Signing our messages.

1. There are some subtle issues in using this RSA system in practice.
2. Since everyone knows how to encrypt messages to us, how can we be certain that a message we receive asserting that it is from Zach is really from Zach? Perhaps it is a forged message sent by Marcy.
3. One way to combat this problem is for the sender to include what is called an *electronic signature*.
4. An electronic signature can be generated using the sender's secret number that no one else knows. This way we can authenticate the authorship of any message we receive.

B. Breaking the code.

1. Is this code unbreakable? No. If we factor the number m that is known to be a product of exactly two primes, then we can find the secret decoding number.
2. Is this factorization approach the only way to break the code? This remains an important open question in cryptography and number theory; namely, is breaking the RSA code equivalent to factoring the number m?
3. From a practical standpoint, even if there does exist some devilishly sneaky and relatively easy way of breaking the RSA code, as long as no one has found it, the coding scheme remains safe.

C. Selecting the prime numbers for RSA.
   1. Even though we have seen that there is no formula known to generate all the primes, there are methods to generate very large primes. Although factoring is very difficult, even for computers, multiplication of enormous numbers is an easy task.
   2. To create an unbreakable RSA scheme, we need only pick two primes so large that no computer on Earth today can factor their product. In practice we probably will not need to use such gigantic numbers.
   3. How large should our primes be? It depends on the value of the information.
   4. Very important information, such as national security memoranda, would warrant extremely large primes.
   5. The date of a surprise birthday party is not quite as important, and thus fewer people might be willing to invest millions of dollars on computing technology to factor the number m and thus break the code. In this case, small primes would certainly suffice.
   6. The idea of placing a value on information was touted by one of the great foremothers of modern computers and computing, Admiral Grace Hopper.
   7. She saw the importance of determining the cost of replacing lost data long before backing up computers and data was in fashion.
   8. She made enormous contributions to computer science, including being one of the architects of the programming language COBOL.

D. Turning a number from small to enormous.
   1. From a number theoretic point of view, the number 400,000,000 is insignificant since almost all natural numbers are larger than it.
   2. However there is a way of transforming this small number into an enormous one—even in the eyes of number theorists. Just insert a dollar sign in front: $400 million.
   3. This was the price paid by Security Dynamics in 1996 to purchase RSA Data Security—the company formed to promote and sell the RSA systems.
   4. Moral: It pays to create number theory theorems.

Questions to Consider:

1. Without performing any calculations at all, find the remainder when 7^4 is divided by 12. Check your answer using a calculator.
2. We saw that one way to break the RSA encryption scheme involves factoring very large numbers, which is possible in theory but impossible in practice with current computer capabilities. What other scenarios can you think of, even beyond number theory, in which something is possible in theory but not in practice?

Lecture Thirteen
Fermat's Method of Ascent

Scope: When most people think of mathematics, their minds drift toward cryptic equations and the need to "solve for x." Here we will study a very broad class of equations known as *Diophantine equations*. These are equations that, in some sense, involve only integers and for which we desire only integer solutions. They are named in honor of the influential 3rd-century Greek mathematician Diophantus of Alexandria. We will begin with his story and the history of these well-studied important equations. Determining whether a Diophantine equation has no integer solutions, finitely many integer solutions, or infinitely many integer solutions is extremely challenging and has become a fine art. Here we will examine the famous, but misnamed, *Pell equation* in order to introduce *Fermat's method of ascent*—an important technique for finding infinitely many solutions to a Diophantine equation. We will close with a brief discussion of a famous metaquestion posed by the great late-19th-century German mathematician David Hilbert, which asked if there exists an algorithm for determining whether or not an arbitrary Diophantine equation has a solution. As we will see here, a complete answer to this question was only found in 1970 and, remarkably, involves the Fibonacci numbers. These algebraic equations open our exploration into algebraic number theory.

Outline

I. Diophantus of Alexandria and his equations.
  A. Diophantus and his passion for arithmetic.
    1. Diophantus of Alexandria was a great mathematician from the 3rd century.
    2. Very little is known about the life of Diophantus outside of a conundrum that appeared in the *Greek Anthology* from 600 C.E.
    3. The puzzle challenged the reader to figure out Diophantus's age when he died. If we let x denote his age, then the puzzle can be translated into the equation $x/6 + x/12 + x/7 + 5 + x/2 + 4 = x$. And if we solve this equation, we find that $x = 84$.
    4. This story and its solution highlight his greatest mathematical passion: searching for natural-number solutions to certain equations.
  B. Contributions to how we view equations today.
    1. Diophantus made enormous contributions to algebra and, in fact, is often referred to as the "Father of Algebra."
    2. He is believed to be the first Greek mathematician to accept rational numbers as numbers.
    3. Moreover, Diophantus is credited for introducing mathematical notation and symbols for solving equations, rather than using prose as was the custom at the time.
    4. He was particularly interested in finding natural-number solutions to certain equations. If a solution turned out to be a fraction, then he would accept that reality. However, Diophantus viewed a negative solution or irrational solution as "useless" or "absurd"—perhaps because his equations often arose from counting objects.
    5. In fact, he once called the equation $4x + 24 = 4$ "absurd" because the answer, $x = -5$, is negative.
  C. His seminal 13 volumes of *Arithmetica*.
    1. Diophantus's most important work was a 13-volume collection of books entitled *Arithmetica*.
    2. Only 6 volumes have been found.
    3. The texts are perhaps the first algebra books ever written, in that algebra questions are posed and the solutions are given using notation that later evolved into our present mathematical symbolic language.
    4. In 1570, Italian mathematician Rafael Bombelli was the first to translate Diophantus's books into Latin.
    5. In the next lecture we will return to Bombelli's 1621 Latin translation in regard to Pierre de Fermat.
  D. Diophantine equations.
    1. Today if we consider an equation and we wish to determine if there exist integer solutions, we call the equation a Diophantine equation.

2. Thus, given a Diophantine equation, our implicit goal is to determine whether there are integer solutions or not. If there *are* integer solutions, then the follow-up questions include: Are there finitely many or infinitely many solutions? Can we find them all?
3. For example, if we consider the Diophantine equation $2x + 1 = 7$, then we can find that there are only finitely many solutions: in fact only one solution, $x = 3$. If we consider the slightly altered equation $2x + 1 = 6$, then we find that there are no *integer* solutions, but there is exactly one *rational* solution: $x = 5/2$.
4. If we consider the equation $x^2 = 16$, then we see that this equation has only finitely many integer solutions (in fact just two solutions): $x = 4$ and $x = -4$. However, if we consider $x^2 = -1$, then this equation has no integer solutions (we require the imaginary number i).
5. If we consider the equation from our lecture on relatively prime integers and the previous lecture on RSA public key cryptography—for relatively prime natural numbers a and b, $ax - by = 1$—then there are infinitely many natural-number solutions.
6. For example, if we consider $3x - 2y = 1$, then for any natural number n, we have the solution $x = 2n + 1$ and $y = 3n + 1$. Here the n can be viewed as a *variable* or as a *parameter*.

II. Determining if a Diophantine equation has integer solutions.

A. Remainders reveal no solutions.

1. All the equations we consider here will be sums, differences, products, and powers of integers and unknowns. The recurring question is, Are there integer solutions?
2. An integer solution will thus give an equality between two integers. Therefore, the left and right sides of the equation must have equal remainders when divided by any particular natural number.
3. However, if we can find a natural number, say m, so that dividing by m gives a different remainder on the left side of the equation from the remainder on the right side, then there cannot be integer solutions to the original equation.

4. For example, we consider the equation $4x = 2y^3 + 1$. Let us assume that there *are* integer values for x and y that satisfy the equation. What if we consider the remainder of both sides of this equation when dividing by 2?
5. The left-hand side is even, so the remainder equals 0, while the right-hand side is odd, so the remainder equals 1. In other words, the remainders are not equal, and therefore it is impossible for the two sides of the equation to be equal *integers*. So there are no integer solutions to this equation.
6. Modular arithmetic can often be used to show that certain Diophantine equations have no integer solutions.

B. The Pythagorean equation.

1. One of the most famous Diophantine equations is the equation that is associated with the all-important Pythagorean Theorem involving right triangles from geometry.
2. We recall the equation $x^2 + y^2 = z^2$. Are there natural-number solutions to this equation?
3. Yes, and a well-known solution is $x = 3$, $y = 4$, and $z = 5$. Are there others? Yes: $(x, y, z) = (6, 8, 10)$, but this is just the previous solution doubled. Are there other, genuinely different, solutions? Yes: 5, 12, 13. These natural-number solutions are known as Pythagorean triples. Are there infinitely many Pythagorean triples? We will return to this question in Lecture Sixteen.

C. The Pell equation.

1. As we have seen, the Pythagorean equation is one that involves squares (powers of 2). Here we look at another collection of famous equations that involve squares.
2. An example of this particular type of equation is $x^2 - 2y^2 = 1$; and more generally for any fixed square-free natural number $d > 1$, we consider the equation $x^2 - dy^2 = 1$.
3. Diophantine equations of this form are called *Pell equations*, named after 17th-century British mathematician John Pell. Unfortunately, Pell really did not study these equations.
4. Gauss mistakenly attributed the study of these equations to Pell, and the name stuck.
5. In fact these equations have been studied for thousands of years.

III. Fermat's method of ascent.

A. One solution generates another one.

1. *Fermat's method of ascent* shows that certain Diophantine equations have *infinitely* many natural-number solutions.

2. His idea is to first find one natural-number solution to the equation at hand and then use that solution to generate another, larger solution.

3. If he repeats this exact procedure with the new solution, then he produces another, still-larger solution.

4. In this manner Fermat finds an endless tower of ever-growing natural-number solutions; hence the name "method of ascent."

B. Returning to Pell's equation.

1. To illustrate Fermat's method of ascent, let us return to the Pell equation $x^2 - 2y^2 = 1$. Notice that $x = 3$ and $y = 2$ are a natural-number solution to this equation. Since this is the first solution we found, let us call these values $x_1 = 3$ and $y_1 = 2$.

2. For any natural n, we define the numbers $x_{n+1} = 3x_n + 4y_n$ and $y_{n+1} = 2x_n + 3y_n$. Notice how these formulas are defined recursively. These are, in some sense, a pair of recurrence sequences. For example, $x_2 = (3 \times 3) + (4 \times 2) = 9 + 8 = 17$, and $y_2 = (2 \times 3) + (3 \times 2) = 12$. Notice that $17^2 - (2 \times 12^2) = 289 - (2 \times 144) = 289 - 288 = 1$; that is, we found another, larger solution to our Pell equation.

3. In general, if we assume that x_n and y_n is a solution to $x^2 - 2y^2 = 1$—that is, $(x_n)^2 - 2(y_n)^2 = 1$—then if we compute $(x_{n+1})^2 - 2(y_{n+1})^2$, we see $(x_{n+1})^2 - 2(y_{n+1})^2 = (3x_n + 4y_n)^2 - 2(2x_n + 3y_n)^2 = 9(x_n)^2 + 24x_ny_n + 16(y_n)^2 - 8(x_n)^2 - 24x_ny_n - 18(y_n)^2 = (x_n)^2 - 2(y_n)^2 = 1$. So we see that x_{n+1} and y_{n+1} is another (larger) solution.

4. This method of ascent can be generalized and can be applied to any Pell equation. Therefore we conclude that all such Pell equations have infinitely many natural-number solutions.

C. Connecting a curve with an equation.

1. In order to foreshadow ideas that we will explore in greater detail in our sojourn into algebraic geometry, we now consider a curve associated with the equation $x^2 - 2y^2 = 1$.

2. If we now consider all decimal numbers (real numbers) that satisfy this Pell equation, then we can plot all those points in the xy-coordinate plane. Those points form the graph of a curve associated with the equation. This particular curve is a shape known as a *hyperbola* and actually has two perhaps scary-looking asymptotes.

3. If we place dots at all the coordinates in which both x and y are integers, then we see a grid-like lattice of points. Asking if there are any natural-number solutions to this equation is equivalent to asking if this curve passes through any of these regular lattice points.

4. It is not obvious that this gently curving graph passes through infinitely many of these integer lattice points, but we have shown algebraically through Fermat's method of ascent that the curve in fact does.

IV. David Hilbert's 10^{th} question.

A. Can every Diophantine equation be "solved"?

1. Hilbert's 10^{th} question can be phrased as: Given a Diophantine equation with any number of unknowns and with integer coefficients, devise a process that will determine in a finite number of operations whether the equation is solvable in integers.

2. In other words, Hilbert asked if there exists an algorithm for determining whether an arbitrary Diophantine equation has an integer solution.

B. A search for an algorithm.

1. Mathematicians studied this most challenging question for 70 years. Finally, in 1970, Russian mathematician Yuri Matiyasevich gave a complete answer: No. There cannot exist a general algorithm that will determine in a finite number of steps if an arbitrary Diophantine equation has an integer solution.

2. His deep proof involved constructing a system of 10 simultaneous equations. Surprisingly, one of the key pieces of his argument involved a delicate and important result involving Fibonacci numbers and recurrence sequences.

C. Further consequences and insights.

1. This question connects number theory with very subtle issues from logic.

2. In fact, many questions that we have already considered, including the Goldbach conjecture and the Riemann Hypothesis, have been shown to be logically equivalent to asking if there are integer solutions to certain complicated systems of Diophantine equations. If the system of Diophantine equations has *no* integer solutions, then the answer to its associated open question is "yes."
3. In some vague sense, every mathematical question involving arithmetic can be converted into a question involving Diophantine equations.

Questions to Consider:

1. By considering remainders after division by 3 of each term, show there are no integer solutions to the Diophantine equation $6x^3 - 9y^2 = 3z + 2$.
2. Use Fermat's method of ascent and the recurrence formula given in the lecture to find a third solution to $x^2 - 2y^2 = 1$.

Lecture Fourteen
Fermat's Last Theorem

Scope: One of the most famous and romantic stories in number theory is the legend known as *Fermat's Last Theorem*. While we have already seen in the previous lecture that there exist natural-number solutions to the Pythagorean equation $x^2 + y^2 = z^2$, Fermat asserted in 1637 that for any fixed natural-number exponent n greater than 2, there are *no* natural-number solutions x, y, and z to the equation $x^n + y^n = z^n$. Fermat penned this assertion in the margin of his copy of Diophantus's treatise *Arithmetica*, along with a cryptic and now infamous reference to its proof. After highlighting the history of this most celebrated equation in mathematics, we will verify that to establish Fermat's claim we need only prove that his equation has no solutions for exponents equal to 4 and equal to all prime numbers beyond 2 using his ingenious *method of descent*—an idea that beautifully mirrors his *method of ascent* described in the previous lecture. There is a long and impressive list of great mathematicians who have made progress toward a solution of Fermat's Last Theorem. Here we will highlight some of the contributions made by Leonhard Euler, Sophie Germain, Johann Dirichlet, and Adrien-Marie Legendre in the 18th century. In the next century, Gabriel Lamé produced what he believed to be a correct and complete proof of Fermat's Last Theorem. However, Ernst Kummer quickly discovered a subtle error in the argument. Kummer's attempt to repair the problem led to an entirely new field of study now known as *algebraic number theory*. Thus we see that while none of these great 18th- and 19th-century minds produced a complete solution to this challenging conundrum of Fermat, they did move the frontiers of number theory forward with their creativity, imagination, and profound insights. A complete proof of Fermat's famous theorem, however, would have to wait until the end of the 20th century. We will see the dramatic conclusion of this story unfold in Lecture Eighteen.

Outline

I. The story of Fermat and his many "theorems."

A. Fermat's first passion.
   1. Recall that Pierre de Fermat was a 17th-century French lawyer who was also a member of the local parliament in Toulouse.
   2. Number theory was a leisure activity to Fermat. He was a gentleman scholar who was somewhat secretive in his work and generally reclusive.

B. Fermat's famous assertions.
   1. Since number theory was Fermat's recreation and he did not publish his results in scholarly journals, he had no obligation to write complete and correct proofs of his mathematical assertions.
   2. Instead he would write notes in the margins of books and describe his mathematical discoveries in letters to mathematicians of the day.
   3. Despite his lack of formal rigor, his insights were remarkable and his contributions to mathematics were enormous. Given his extraordinary mathematical creativity and originality, the mathematical community has forgiven his cavalier treatment of the rigors of proof.
   4. Others that followed Fermat could either produce counterexamples to those assertions that were not true in general or provide mathematical proofs to those assertions of Fermat that were in fact theorems.
   5. Over many subsequent years, all of Fermat's assertions were resolved one way or another—all but one last assertion. Because it was the last assertion that remained open, it became known as Fermat's Last Theorem.

C. The inspirational words of Diophantus.
   1. Fermat studied the Latin translation of Diophantus's *Arithmetica* with great care, writing many notes in the margin of his copy.
   2. Question II.8 in *Arithmetica* asked how to express a given square natural number as the sum of two other square natural numbers. In other words, the Pythagorean equation $x^2 + y^2 = z^2$. We will study this equation for ourselves in Lecture Sixteen.
   3. It was this question of Diophantus that inspired Fermat, around the year 1640, to write down the most famous Diophantine equation in number theory.

II. The most famous Diophantine equation.

A. Moving beyond the exponent 2 and extending the Pythagorean equation.
   1. In the margin, Fermat wrote, in Latin, the most famous marginal note in the history of mathematics. Translated, he wrote: "It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second into two like powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain."
   2. Fermat's assertion in the margin can be stated formally as: Given any fixed natural number $n > 2$, there are no natural numbers x, y, and z that satisfy the Diophantine equation $x^n + y^n = z^n$.

B. Fermat's infamous "Last Theorem."
   1. Because this was the last assertion to be verified or disproved, it became known as Fermat's Last Theorem.
   2. To disprove his claim, we need only find a natural number $n > 2$ for which the Diophantine equation $x^n + y^n = z^n$ has natural-number solutions.

III. A focus on 4 and the odd primes.

A. Examining the exponents.
   1. Fermat's Last Theorem is a statement that the Fermat equation has no natural-number solutions for *all* exponents greater than 2. So it is, in fact, infinitely many statements: a statement for $n = 3, 4, 5, 6, 7, 8, \ldots$. We first ask if we need to prove *all* these cases.
   2. In order to analyze this question, we first review an important property of exponents. Specifically, we notice that $x^6 = (x^2)(x^2)(x^2) = (x^2)^3$. More generally, if the natural number n can be factored as $n = ab$, then $x^n = (x^a)^b$.
   3. Using this property, we claim we need only prove Fermat's Last Theorem for the cases in which $n = 4$ and n equals an odd prime number (3, 5, 7, 11, 13, ...). That is, there is no need to check any other composite exponents other than 4. This claim would certainly reduce the number of exponents to verify.
   4. Why is this claim true? Suppose that we *have* established Fermat's Last Theorem for all odd prime exponents and the

exponent 4. That is, we will assume that for any of these exponents we know there are no natural-number solutions to Fermat's equation.

5. We now consider composite exponents greater than 2. For example, we consider $n = 6$. If we assume that there *is* a natural-number solution to $x^6 + y^6 = z^6$, then by our property of exponents, we can rewrite this as the equivalent equation $(x^2)^3 + (y^2)^3 = (z^2)^3$.
6. Now since x, y, and z are natural numbers, so are their squares. That is, we have just found natural-number solutions to the Fermat equation with $n = 3$, an odd prime. This contradicts our hypothesis that there are no solutions. Therefore we must have no natural-number solutions for the exponent 6 as well.
7. Suppose we now consider the exponent 8. If we assume that there *is* a natural-number solution to $x^8 + y^8 = z^8$, then again by our property of exponents, we can rewrite this as the equivalent equation $(x^2)^4 + (y^2)^4 = (z^2)^4$, which again yields a contradiction, since there are no natural-number solutions for the exponent 4. Hence there cannot be natural-number solutions for the exponent 8.
8. This argument works for all composite natural-number exponents greater than 2. If we have a composite natural number greater than 2, then it either must have an odd prime factor *or* it must have a factor of 4. In either case, by our hypothesis that the result holds for 4 and all the odd primes, we conclude that Fermat's Last Theorem must hold for all natural number exponents greater than 2.
9. Thus we have proved that it is enough to just consider special exponents: the numbers 4 and all the odd primes.

B. Fermat's method of descent.

1. Fermat himself devised an ingenious method to prove that his equation has no natural-number solutions for the exponent $n = 4$.
2. He called this method the method of descent, and it mirrors his method of ascent that we described in the previous lecture.
3. In the method of descent, we assume that we have a natural-number solution to a Diophantine equation. Using this assumed solution, we construct a *smaller* natural-number solution. We can then repeat the process again with this smaller solution.
4. In fact we can repeat this process indefinitely and thus create an arbitrarily long chain of natural numbers that are getting smaller and smaller. However there are only finitely many natural numbers smaller than any given number.
5. This conclusion leads us to a contradiction, and thus our assumption that a first such natural-number solution existed must be false. Hence there are no natural-number solutions to the original Diophantine equation.
6. We again see the "divide and conquer" theme in Fermat's method of descent.
7. This method turns out to be extremely useful and can be applied to a variety of mathematical issues.

C. Reducing the issue down to the prime numbers.

1. Using this method in a most clever way, Fermat was able to prove that there are no natural-number solutions to the Diophantine equation $x^4 + y^4 = z^2$.
2. Using this result, if we assume that there were natural-number solutions to $x^4 + y^4 = z^4$, then we could write it as $x^4 + y^4 = (z^2)^2$. That is, we see that x, y, and z^2 is a natural-number solution to $x^4 + y^4 = z^2$, which is impossible. Hence there are no natural-number solutions to Fermat's equation with $n = 4$.
3. Thus we need only prove that Fermat's Last Theorem is true for all odd prime exponents—still a tall order, indeed.

IV. An 18th- and 19th-century struggle to find a proof.

A. Leonhard Euler and $n = 3$.

1. Leonhard Euler was able to adopt Fermat's method of descent to prove that Fermat's equation had no natural-number solutions for $n = 3$.
2. There were some small errors and gaps in Euler's work, but those were all repaired by applying other results of Euler himself.
3. His proof generated much interest in this question.

B. Sophie Germain's clever new approach.

1. Sophie Germain, born April 1, 1776, was inspired to become a mathematician when, at the age of 13, she read about Archimedes.

2. Early on, she would submit papers and write letters under the pseudonym Monsieur Le Blanc. After Gauss, one of her supporters, discovered that Monsieur Le Blanc was in fact a female author, he wrote that "... she must have the noblest courage, quite extraordinary talents, and superior genius."
3. She produced a number of extremely important results in number theory. In fact, one of them led to the concept of what are now called *Germain primes*. A prime number p is a Germain prime if the number $2p + 1$ is also prime. For example, 3 is a Germain prime since $2 \times 3 + 1 = 7$ is also prime. However, 7 is not a Germain prime, since $2 \times 7 + 1 = 15$, which is not prime.
4. One of Germain's most important discoveries was connected with Fermat's Last Theorem. She proved the very deep theorem that asserts: If x, y, and z are natural numbers that satisfy $x^5 + y^5 = z^5$, then 5 must be a factor of either x, y, or z.

C. Crossing 5 and 7 off our list.
1. In 1825, Dirichlet and Legendre used the ideas of Germain and generalized the arguments of Euler to prove that Fermat's Last Theorem is true for the exponent 5.
2. In 1839, French mathematician Gabriel Lamé offered a very lengthy proof of Fermat's Last Theorem for the prime exponent 7. His argument was so complicated that it did not appear as if it could be extended to other primes.

V. A wonderful mistake of Lamé's.

A. Gabriel Lamé's other announcement of 1839.
1. Later in 1839, Lamé claimed he had a complete proof of Fermat's Last Theorem for all odd primes.
2. Sadly, despite the fact that his ideas were very clever, there was an error in his argument.
3. In fact since that point, there have been literally thousands of false proofs of Fermat's Last Theorem (authored by both mathematicians and nonexperts).

B. Ernst Kummer's response.
1. It was the German mathematician Ernst Kummer who quickly noticed the subtle error in Lamé's work.
2. Since Lamé's idea was so clever, Kummer attempted to patch up the proof. Although his work did not complete the proof of Fermat's Last Theorem, it did provide the foundations for an entirely new branch of number theory—now known as *algebraic number theory*.
3. In 1847, Kummer extended the ideas of Euler, Germain, Dirichlet, Legendre, and others to prove that Fermat's Last Theorem is true for all so-called regular prime exponents. A "regular prime" is a prime that satisfies some very complicated algebraic properties that we will not describe here.
4. If we consider all the primes less than 100, then it has been shown that all of these primes are regular *except* for the primes 37, 59, and 67. Thus, from this small evidence, it would appear that most primes are regular.
5. It is conjectured that approximately 61% of all primes are regular primes.
6. However, it remains an open question to determine if there are *infinitely many* regular primes!

C. A complete and correct proof.
1. In spite of all these great contributions from outstanding minds from the 18th and 19th centuries, a complete proof of Fermat's Last Theorem would have to wait until the end of the 20th century.
2. In the early 1990s, Andrew Wiles finally gave a correct and complete proof of this 350-year-old open question. This dramatic conclusion of this epic number theoretic saga will have to wait until Lecture Eighteen.

Questions to Consider:

1. Suppose that there are no natural numbers x, y, and z that satisfy $x^5 + y^5 = z^5$. Using this assumption, show that there are no natural numbers x, y, and z that satisfy $x^{100} + y^{100} = z^{100}$.
2. The prime number 11 is a Germain prime since $2 \times 11 + 1$ (which equals 23) is also prime. Find the next Germain prime after 11.

Lecture Fifteen
Factorization and Algebraic Number Theory

Scope: As we have seen earlier in the course, the fact that every natural number greater than 1 can be factored *uniquely* into a product of prime numbers is an ancient and fundamental theorem upon which all of basic number theory rests. In this lecture we will return to this ancient notion of *unique factorization*, first proved by Euclid, and discover some of its important ramifications within the realm of Diophantine equations. We then will challenge our imagination to consider a world of number that *does not* exhibit the property of unique factorization into primes. The reality that some collections of numbers can be factored into primes in more than one way is at once surprising and revealing. These discoveries will lead us to the notions of algebraic integers and generalized prime numbers. Armed with these new ideas, we will describe Gabriel Lamé's failed strategy to prove Fermat's Last Theorem and offer an overview into the theory of Ernst Kummer that was inspired by Lamé's failed attempt. This stunning and powerful theory gave birth to what we today call *algebraic number theory*. Given that this important area of number theory has its roots in factorization properties, it is perhaps not surprising that these abstract ideas now have practical implications in the modern theory of cryptography.

Outline

I. Euclid's unique prime factorization, revisited.
  A. Euclid's fundamental theorem of arithmetic.
    1. We recall Euclid's famous result, now known as the *fundamental theorem of arithmetic*.
    2. It states that every natural number greater than 1 can be expressed as a product of prime numbers and, moreover, that this factorization, except for possible rearrangement of the factors, is unique.
    3. We proved that every natural number greater than 1 can be expressed as a product of primes by adopting a "divide and conquer" method. For example, $12 = 2 \times 6 = 2 \times 2 \times 3$.
    4. We did not prove the uniqueness of this factorization. In our previous example, we have $12 = 2 \times 2 \times 3 = 2 \times 3 \times 2 = 3 \times 2 \times 2$. As intuitive as the uniqueness feature might appear, we will soon see that this property should not be taken for granted.
  B. Finding all solutions using unique factorization.
    1. We can apply the fundamental theorem of arithmetic to find integer solutions to certain Diophantine equations.
    2. To illustrate this method, we consider the Diophantine equation $x^2 - y^2 = 5$.
    3. Note that the left side of this equation can be factored: $x^2 - y^2 = (x + y)(x - y) = 5$. However, since 5 is a prime, the only possible pairs of integers whose product is 5 are 5 and 1, 1 and 5, -5 and -1, and lastly -1 and -5.
    4. If we consider the first pair, we obtain the pair of simultaneous equations $x + y = 5$ and $x - y = 1$. If we add these equations together, we discover that $2x = 6$, and thus $x = 3$. If $x = 3$, then we see that $y = 2$. Hence we found an integer solution (note that $3^2 - 2^2 = 9 - 4 = 5$).
    5. Considering the other cases, we find that all solutions are given by $x = \pm 3$ and $y = \pm 2$, so there are exactly four integer solutions to this equation.
  C. Proving there are no solutions via unique factorization.
    1. Unique factorization into primes also allows us to demonstrate that certain Diophantine equations have *no* integer solutions.
    2. To illustrate this method, we consider a modified version of the previous Diophantine equation, $x^2 - y^2 = 6$.
    3. We again factor the left side to see that $x^2 - y^2 = (x + y)(x - y) = 6$. In this case, there are many ways to factor 6 into two factors. In particular, $6 = 1 \times 6 = 2 \times 3 = 3 \times 2 = 6 \times 1$. If we consider each of these possible factorizations, we will discover that they lead to no integer solutions.
    4. For example, let us consider the possibility that $x + y = 3$ and $x - y = 2$. If we add these equations together, we discover that $2x = 5$ and hence $x = 5/2$, which is not an integer. Similarly, we can check that the three other possible factorizations do not lead to any integer solutions. Hence this equation has no integer solutions.

5. These methods show us the power of unique factorization of numbers into primes as applied to solving Diophantine equations.

II. A number world without unique factorization.

A. Celebrating the arithmetic structure of the integers.

1. Within the context of Diophantine equations and beyond, we have seen the power of the arithmetical structure of the integers.
2. Beyond the all-important property of factorability into fundamental building blocks (the primes), the integers satisfy many axioms of arithmetic that we take for granted as we solve equations.
3. For example, the sum of any two integers is an integer; there exists an additive identity element—namely 0; and for any integer, there exists another integer (called the additive inverse) so that their sum equals 0 (we call this second number the negative of the first). For example, $3 + (-3) = 0$. Moreover, we can group numbers in any way to add them up; for example: $3 + 5 + 2 = (3 + 5) + 2 = 3 + (5 + 2) = 10$. This property is called associativity of addition.
4. Of course we also have multiplication. The product of any two integers is again an integer, and multiplication is also associative. Furthermore, multiplication and addition work together through what we call the distributive laws that include $a(b + c) = ab + ac$.
5. These properties allow us to solve simple algebraic equations such as $x + 5 = 7$. Any collection of numbers that satisfies all these properties is called a *ring*—the abstraction of the integers, studied in great depth in what is called *abstract algebra*.

B. A world of even numbers.

1. We now consider an entirely new universe of number—one with which we are already familiar: the collection of all even integers: 2, 4, 6, 8, … , together with their negatives and zero. For now we will view this collection of numbers as our entire universe of numbers; we will pretend here that the odd numbers do not exist.
2. We can check that the collection of all even numbers is another example of a ring: If we add or multiply two even numbers, we get an even number; those operations are associative; they satisfy the distributive properties; we have the additive identity 0; and every number has an additive inverse (for example, −10 is the additive inverse of 10).

C. Even prime numbers.

1. We can now consider the "prime numbers" within this context of number. That is, those even numbers that cannot be factored any further into the product of numbers from our collection.
2. Of course 2 is a prime, but now we see some new primes as well. For example, now 6 is "prime" since we cannot factor 6 into the product of two smaller *even* numbers! The number 12 is not prime, since it can be written as 2×6 (two even numbers).
3. Thus the first few "prime numbers" within the even-number universe are 2, 6, 10, 14, 18, 22, and so forth. Notice, for example, that 20 is composite, since it can be expressed as 2×10.

D. Unique factorization fails.

1. Adopting the "divide and conquer" strategy we previously employed, we can quickly discover that every even number is either a prime or can be expressed as a product of even primes.
2. However, do we still have uniqueness of prime factorization?
3. Let us consider the factorization of 24. It can be expressed as $2 \times 2 \times 6$ (all "primes"), and except for the rearrangement of factors, this product is unique.
4. Let us now consider the factorization of 36. It can be expressed as 6×6 (two "primes"). However, it can also be expressed as 2×18, and 18 is in fact a "prime." Thus we see two different factorizations into primes.
5. Hence we conclude that this ring of numbers does not exhibit the *unique* factorization into primes.

III. An introduction to algebraic integers.

A. A further generalization of the integers.

1. While the ring of even integers—a ring that we just discovered does not enjoy the property of unique factorization into primes—is not particularly useful in practice within the

study of number theory, there are other rings of integers that are extremely important.

2. These new rings of integers generalize the ring of ordinary integers in a different direction. These rings grow out of complicated solutions to certain special equations.
3. For example, if we consider the solutions of the equation $x^2 = -5$, then we see that $x = \pm\sqrt{(-5)}$, two imaginary numbers. We can use $\sqrt{(-5)}$ to create an entirely new ring of integers that includes the traditional ones.
4. We consider the collection of all numbers of the general form $a + b\sqrt{(-5)}$, in which the numbers a and b are ordinary integers. So for example, $2 + 3\sqrt{(-5)}$; $-1 + 8\sqrt{(-5)}$; $-19\sqrt{(-5)}$, which can be written as $0 + -19\sqrt{(-5)}$; and even 7, which can be expressed as $7 + 0\sqrt{(-5)}$, are all examples of "integers" in this new collection of numbers.
5. It can be shown that this collection satisfies all the properties required to make it a ring, and thus we can view it as a generalized ring of integers. This collection is an example of what is known as a ring of algebraic integers.

B. Primes and unique factorization.

1. Just as with the ordinary integers and with the even integers, we can identify the prime numbers within this ring—that is, the fundamental multiplicative building blocks within this collection of algebraic integers.
2. Identifying which numbers are primes and which are composite is tricky business here. For example, some primes look like regular primes (such as 3 and 7); however, other primes look more exotic. For example, the numbers $1 + 2\sqrt{(-5)}$ and $1 - 2\sqrt{(-5)}$ are both primes in our new ring of algebraic integers.
3. Using a much more elaborate "divide and conquer" technique, it has been shown that every algebraic integer in such a ring is the product of primes.
4. However, in general we cannot guarantee the *uniqueness* of this factorization into primes for a ring of algebraic integers.
5. For example, in our ring involving $\sqrt{(-5)}$'s, we can see that the number $21 = 3 \times 7$ (the product of two primes). However, we now claim that 21 also equals $1 + 2\sqrt{(-5)}$ times $1 - 2\sqrt{(-5)}$—that is, the product of two other primes.
6. To confirm this assertion, we multiply: $(1 + 2\sqrt{(-5)})(1 - 2\sqrt{(-5)}) = 1 + 2\sqrt{(-5)} - 2\sqrt{(-5)} - 4(\sqrt{(-5)})^2 = 1 + 0 - 4(-5) = 1 + 20 = 21$.
7. Therefore we see that this ring of algebraic integers does not possess the unique factorization property.

IV. Lamé's failed factorization proof.

A. Factoring the Fermat equation.

1. We recall that in 1839 Gabriel Lamé produced a very elaborate argument to prove Fermat's Last Theorem in the case $n = 7$; that is, he proved that the Diophantine equation $x^7 + y^7 = z^7$ has no natural-number solutions.
2. That same year he announced that he had proved Fermat's Last Theorem in general. That is, for any natural number n greater than 2, the equation $x^n + y^n = z^n$ has no natural-number solutions.

B. A proof assuming unique factorization.

1. His idea was to assume that there were integer solutions and then factor the equation. Recall, for example, our proof that the equation $x^2 - y^2 = 6$ has no natural-number solutions. We factored $(x + y)(x - y) = 6$ and saw that there could not be a factorization of 6 that satisfied this equation.
2. However to factor Fermat's equation, Lamé had to use algebraic integers (rather than just the ordinary integers).

C. A fatal assumption.

1. After he factored Fermat's equation using numbers from a certain ring of algebraic integers, he assumed that this ring of algebraic integers possessed the property of unique factorization into primes that the ordinary integers enjoy.
2. Given this assumption of unique factorization, Lamé's proof was correct. However, the question remained, Did Lamé's ring of algebraic integers possess this unique factorization property? We have just seen an example of such a ring that did not satisfy this property.

3. Unfortunately for Lamé, his ring of algebraic integers *did not* possess the unique factorization property, and thus his proof was flawed.

V. Kummer's discovery of "ideal numbers."
   A. The factorization problem with Lamé's proof was quickly found by Ernst Kummer.
   B. Trying to salvage Lamé's idea.
      1. Kummer tried hard to fix the problem with Lamé's proof since it was otherwise a clever strategy for attacking Fermat's Last Theorem.
      2. The question remained, Is there a way to capture some essence of unique factorization into primes within all rings of algebraic integers?
      3. Kummer then made a marvelous discovery about algebraic integers.
   C. Kummer's new notion of "ideal numbers."
      1. Kummer proved that even though there can be rings of algebraic integers that do not possess unique factorization into primes, every such ring can be cut up into packets of numbers—small collections of algebraic integers.
      2. These collections can be combined with operations similar to addition and multiplication and, in fact, form a ring. That is, we can perform arithmetic, but instead of performing the arithmetic with pairs of numbers, Kummer suggested that we perform arithmetic with pairs of packets of numbers.
      3. He then found that within these packets of numbers there are prime elements—fundamental multiplicative building blocks—and proved an amazing result: Every packet can be expressed as a product of these prime packets, and moreover, that factorization is *unique*! In other words, Kummer found a unique factorization property within any ring of algebraic integers—not within the elements themselves but within these packets of elements.
      4. He called these packets of numbers ideal numbers since they enjoyed unique factorization into prime ideal numbers. Today we call these packets "ideals."
      5. Unfortunately the unique factorization into prime ideals was not enough to finish the proof of Fermat's Last Theorem.

   D. The birth of modern algebraic number theory.
      1. Kummer's work launched an entirely new branch of number theory now known as algebraic number theory.
      2. His work had far-reaching consequences in a variety of related and unrelated areas.
      3. In fact, algebraic number theory has connections with cryptography since, as we have seen earlier, encryption issues involve factorization into primes.
      4. Thus Lamé's problematic proof was extremely valuable in inspiring Kummer's groundbreaking work, which did not resolve the issue for which it was intended but did change the face of number theory forever.

Questions to Consider:

1. Returning to the ring of even integers, in how many different ways can you factor 100 into "prime" even integers?
2. Can you think of other important moments in history in which a failed attempt resulted in an important new discovery or insight?

Lecture Sixteen
Pythagorean Triples

Scope: As we have just seen, the epic drama of Fermat's Last Theorem opened with Fermat's inspiration from the words of Diophantus. Those inspirational words arose from a discussion of one of the most important and well-known Diophantine equations—the equation connected with the famous theorem of Pythagoras involving the lengths of the sides of right triangles. Natural number solutions to this equation, $x^2 + y^2 = z^2$, are now known as *Pythagorean triples*. In this lecture we celebrate the history and importance of the Pythagorean Theorem and discover an elegant geometric proof of this ancient result. We will then embark upon a search for Pythagorean triples. Within the Pythagorean triples themselves we will find another surprising appearance of the famous Fibonacci numbers. We will close this lecture with an important connection between Pythagorean triples and particular points on a circle called rational points. This important relationship between numbers and geometry foreshadows our lectures on algebraic geometry—a magnificent modern area of study that not only provides a deeper understanding into the theory of numbers, but also, at long last, leads to a complete solution to Fermat's Last Theorem.

Outline

I. Pythagoras and right triangles.

A. A multicultural fascination with right triangles.

1. The Pythagorean Theorem asserts that given the lengths of the sides of a right triangle (two legs and the hypotenuse), the sum of the squares of the two legs equals the square of the hypotenuse.

2. Put informally, we say that the square on the hypotenuse equals the sum of the squares on the other two sides. This also offers us a visual way of interpreting the result in terms of areas of squares.

3. This result was perhaps first recorded in China around 500 B.C.E. There is also evidence that this result was at least implicitly if not explicitly used in Egypt around 2500 B.C.E. and Mesopotamia around 1750 B.C.E. Many years later the Pythagorean Brotherhood independently rediscovered the result, and since that time, it bears Pythagoras's name.

4. One of the most famous right triangles is the 3-4-5 right triangle, and we can use it to illustrate the Pythagorean Theorem in this special case.

B. An ancient geometric proof without algebra.

1. There are literally hundreds of different proofs of the Pythagorean Theorem.

2. Most are algebraic or geometric in nature.

3. Even a future president of the United States discovered a new proof of this ancient theorem. While serving as a member of the House of Representatives in 1876, James Garfield created his novel proof.

4. Here we now consider the 12th-century geometric proof of the Pythagorean Theorem attributed to the great Indian mathematician Bhaskara. It exemplifies the aesthetics and beauty within mathematical arguments.

C. The converse of the Pythagorean Theorem.

1. We also note that the converse of the Pythagorean Theorem is itself a theorem.

2. That is, if we have a triangle in which the sum of the squares of the lengths of two sides of the triangle equals the square of the length of the third side, then that triangle must be a right triangle.

3. This theorem has a number of practical applications, such as in carpentry.

II. A search for Pythagorean triples.

A. Right triangles having natural numbers as lengths.

1. People throughout human history have been fascinated with right triangles whose lengths are all natural numbers. For example, such right triangles were incorporated in several megalithic monuments found in Egypt and the British Isles from as early as 2500 B.C.E.

2. One famous example is the 3-4-5 right triangle. Another is the 5-12-13 right triangle.

B. Pythagorean triples.

1. Suppose we have a right triangle in which each side length is equal to a natural number. Then the natural-number triple of lengths is called a *Pythagorean triple*.
2. So (3, 4, 5) and (5, 12, 13) are two examples of Pythagorean triples.
3. The famous Mesopotamian stone tablet now known as *Plimpton 322*, from around 1750 B.C.E., contains a long list of Pythagorean triples.

C. Infinitely many Pythagorean triples via factoring.

1. We now prove that there are infinitely many Pythagorean triples, and moreover, we give an algorithm for generating them. The triple (x, y, z) is a Pythagorean triple if x, y, and z are all natural numbers satisfying $x^2 + y^2 = z^2$.
2. We first claim that x, y, and z cannot *all* be odd numbers.
3. Thus we assume that y is an even number, and we write it as $y = 2ab$ for any natural numbers a and b. Solving for y^2, we obtain $y^2 = z^2 - x^2$.
4. We can now factor the right-hand side as we did in the previous lecture to find $y^2 = (z + x)(z - x)$. We also have that $y^2 = (2ab)^2 = (2a^2)(2b^2) = (z + x)(z - x)$.
5. Setting these factors equal, we see that $z + x = 2a^2$, and $z - x = 2b^2$. When we add these two equations together, we see that $2z = 2a^2 + 2b^2$, which simplifies to $z = a^2 + b^2$. If we subtract these two equations, we see that $2x = 2a^2 - 2b^2$, which reduces to $x = a^2 - b^2$.
6. So if we select *any* natural numbers a and b, with a larger than b, and define $y = 2ab$, $x = a^2 - b^2$, and $z = a^2 + b^2$, then (x, y, z) is a Pythagorean triple.
7. For example, if we let $a = 2$ and $b = 1$, then we rediscover the 3-4-5 right triangle. If we now let $a = 5$ and $b = 2$, then we find $x = 21$, $y = 20$, and $z = 29$. Notice that $21^2 + 20^2 = 441 + 400 = 841 = 29^2$; that is, we see that (21, 20, 29) is another Pythagorean triple.
8. Since we have infinitely many different choices for the natural numbers a and b, we see that there are infinitely many genuinely different Pythagorean triples.

III. Another surprising appearance of the Fibonacci numbers.

A. The recurring Fibonacci numbers and Pythagorean triples.

B. Four Fibonacci numbers become one Pythagorean triple.

1. To begin, we select any four consecutive Fibonacci numbers. For illustrative purposes, we consider 1, 2, 3, and 5.
2. We let x equal the product of the outer two numbers, in this case, $x = 1 \times 5 = 5$; we let y equal twice the product of the inner two numbers, in this case, $y = 2 \times (2 \times 3) = 12$; and finally, we let z equal the sum of the squares of the two inner numbers, in this case $z = 2^2 + 3^2 = 4 + 9 = 13$.
3. The triple we just generated will always be a Pythagorean triple. In our example, we found the Pythagorean triple (5, 12, 13).

C. Recurrences generate infinitely many Pythagorean triples.

1. In fact, we could also use any four consecutive Lucas numbers in the same manner, and they will generate a Pythagorean triple.
2. Thus we see that certain recurrence sequences will generate infinitely many Pythagorean triples.
3. Again we see hidden structure—this time within recurrence sequences and Pythagorean triples—amazing connections that bring together seemingly disparate numerical notions.

IV. Finding points on a circle of radius 1.

A. Dividing by z^2 and a formula for a circle.

1. We close this lecture by foreshadowing what lies ahead in our journey.
2. We recall a possibly lost fact from our algebra and geometry days: The formula $X^2 + Y^2 = 1$ describes the graph of a circle of radius 1 centered at the origin (0, 0) of the coordinate plane. This circle is often called the unit circle.
3. We consider a Pythagorean triple (x, y, z) and return to its famous defining equation, $x^2 + y^2 = z^2$.
4. If we divide both sides of the Pythagorean equation by z^2, we obtain $(x/z)^2 + (y/z)^2 = 1$.
5. So we conclude that if (x, y, z) is a Pythagorean triple, then the pair $(x/z, y/z)$ is a point on the graph of the circle of radius 1 centered at (0, 0).

B. From natural numbers to rational numbers.

1. Notice that since x, y, and z are all natural numbers, x/z and y/z are both rational numbers (fractions).
2. Therefore we see that a Pythagorean triple leads to what is called a rational point on the unit circle.
3. For example, if we return to the Pythagorean triple (3, 4, 5), then we see that (3/5, 4/5) is a rational solution to $X^2 + Y^2 = 1$. Notice that $(3/5)^2 + (4/5)^2 = 9/25 + 16/25 = 25/25 = 1$.
4. This observation implies that the point (3/5, 4/5) is on the unit circle.

C. Looking at rational points on the circle.

1. We have closed this lecture with another intriguing and surprising connection of ideas: Each Pythagorean triple can be associated with a rational point on the unit circle.
2. In the next lecture we will see that this connection works in the other direction as well: Each rational point on the unit circle can be associated with a Pythagorean triple.
3. Thus we will connect the question of finding integer solutions to certain Diophantine equations to the question of finding rational points on certain curves.

Questions to Consider:

1. Find an item in your home that you believe contains a right angle. Confirm this by marking 3 inches from the corner in one direction and 4 inches from the corner in the other direction. Then measure the distance between the marks. What should the result be to confirm the angle is a right angle? Is your angle a 90° angle?
2. Think of your favorite natural number greater than 1. Now consider the triple of numbers obtained from the following three steps: Double your favorite, square your favorite and subtract 1, square your favorite and add 1. Verify that this triple is a Pythagorean triple. Can you use this method to show that there are infinitely many Pythagorean triples?

Lecture Seventeen
An Introduction to Algebraic Geometry

Scope: In this lecture we will offer an intuitive introduction into the basic ideas that underlie the seminal branch of number theory known as *algebraic geometry* by discovering a geometric argument that identifies all the Pythagorean triples. This geometric method will involve intersecting the unit circle with a certain collection of lines. Those points of intersection will give way to the Pythagorean triples we seek. Of course, along the way we will review the basic principles and properties of lines and circles in the plane. These deep ideas linking algebra and geometry can be traced back to the ancient Greeks and are connected to the notion of conic sections—the geometric shapes created by slicing an ice-cream-cone-like surface with a plane. These subtle shapes, including circles, ellipses, parabolas, and hyperbolas, can all be described by certain quadratic equations. The fact that we can study these objects both geometrically and algebraically forms the foundation for algebraic geometry.

Outline

I. Pythagorean triples and rational points on a circle.

A. Right triangles with natural numbers as lengths.

1. We recall that a Pythagorean triple is a triple of natural numbers that correspond to the lengths of a right triangle.
2. For example, (3, 4, 5) and (5, 12, 13) are each Pythagorean triples.

B. An algebraic bridge.

1. Suppose that (x, y, z) is a Pythagorean triple. Then we know not only that those three values are natural numbers, but also that they form a solution to the Diophantine equation $x^2 + y^2 = z^2$.
2. Since z is a positive integer, we can divide both sides of this equation by z^2.
3. When we divide, we see $(x/z)^2 + (y/z)^2 = 1$. We also notice that x/z and y/z are rational numbers, so we find that the pair of

rational numbers $(x/z, y/z)$ is a solution to the equation $X^2 + Y^2 = 1$.

4. A natural-number solution to the Pythagorean equation leads to a rational number solution to $X^2 + Y^2 = 1$.
5. For example, the Pythagorean triple (5, 12, 13) leads to the rational solution (5/13, 12/13) to $X^2 + Y^2 = 1$.

C. The unit circle and rational points.

1. If we consider the coordinate plane and plot all the numbers (X, Y) that satisfy the equation $X^2 + Y^2 = 1$, then we would see the graph of a circle centered at the origin, (0, 0), and having radius 1. It is easy to see that $(\pm 1, 0)$ and $(0, \pm 1)$ are four points on the graph. From our previous observations, we also see that $(\pm 3/5, \pm 4/5)$ and $(\pm 5/13, \pm 12/13)$ are eight other points on the graph. We can see that these points fit perfectly on the circle.
2. The circle having radius 1 and centered at the origin, (0, 0), is called the unit circle.
3. We say that a point on the circle is a rational point if both coordinates are rational numbers. So (5/13, 12/13) is a rational point on the unit circle.
4. We have that each Pythagorean triple (x, y, z) leads to a rational point on the unit circle, namely $(x/z, y/z)$. This correspondence also holds in the other direction; that is, rational points on the unit circle lead to Pythagorean triples.
5. For example, the rational point (7/25, 24/25) is a rational point on the unit circle (notice that $(7/25)^2 + (24/25)^2 = 49/625 + 576/625 = 625/625 = 1$). This point corresponds to the Pythagorean triple (7, 24, 25).
6. So we discover this correspondence—or "dictionary"—between rational points on the unit circle and Pythagorean triples. Therefore, to find all Pythagorean triples is equivalent to finding all rational points on the unit circle.

II. A study of lines in the plane.

A. The simplest graphs.

1. Circles are supremely symmetric but possess a graceful curvature that makes them at once alluring and complex.

2. We now consider the simplest graphs imaginable. Those would be graphs that have no curvature at all—the straight line.
3. While the equation of the unit circle involves squares, $X^2 + Y^2 = 1$, the equations for straight lines we will consider look like $Y = 3(X + 1)$, $Y = -8(X + 1)$, or $Y = (2/5)(X + 1)$.
4. We notice that there are no squares appearing in these formulas, and that is why the graphs are straight lines. We also observe that each of these lines share a common point, $X = -1$ and $Y = 0$, denoted as $(-1, 0)$.

B. Graphing lines in the Cartesian plane.

1. Because a straight line is uniquely determined by knowing just two points, to graph a line given its equation, we need only find two points.
2. For example, if we consider the line given by $Y = 3(X + 1)$, we have already seen that it contains the point $(-1, 0)$. If we let $X = 1$, then we see that $Y = 6$, so (1, 6) is another point. If we connect those two points, we find the graph of the line.
3. If we consider the line given by $Y = -8(X + 1)$, we again know that it contains the point $(-1, 0)$. If we let $X = 1$, then now we see that $Y = -16$, so $(1, -16)$ is another point. If we connect those two points, we find the graph of this line.
4. Finally, if we consider the line given by $Y = (2/5)(X + 1)$, we know that it contains the point $(-1, 0)$. If we again let $X = 1$, then we see that $Y = 4/5$, so (1, 4/5) is a second point. If we connect those two points, we find the graph of this line.

C. The notion of slope.

1. As we look at the graphs of these three lines, we notice two features. The first is that they all pass through the point $(-1, 0)$. The second is that the number multiplying the $(X + 1)$ term affects the pitch of the line.
2. The pitch of a line is called the slope, and it is precisely defined as the ratio of the change in the vertical direction to the change in the horizontal direction. That ratio, the slope of a line, is usually denoted as m. The larger the m, the steeper the line is.
3. If m is positive, then the line heads upward as it moves right. If m is negative, then the line heads downward as it moves to the right.

4. Given this notation, we can describe the type of lines we will explore in general by the generic equation $Y = m(X + 1)$, where the m represents the line's slope.
5. The key point is that altering m is equivalent to altering the slope, or pitch, of the line.

III. The main idea behind algebraic geometry.

A. The intersection of lines and circles.

1. If we now consider the unit circle together with our straight lines that pass through the point $(-1, 0)$, then we see that these two graphs intersect at exactly two points: the previously known point, $(-1, 0)$, which is the westernmost point on the unit circle; and a second point.
2. The reason why there are exactly two points of intersection is because the equation for the circle is quadratic: It has powers of 2 and no larger powers. The exponent 2 is what yields the two solutions.
3. We can find the second point of intersection precisely in terms of the slope, m. So we will view the slope m as a fixed but unknown number.

B. An algebraic solution.

1. We can find that second point by solving the two equations $Y = m(X + 1)$ and $X^2 + Y^2 = 1$ simultaneously. We solve these by replacing the Y in the formula for the circle by what it equals in the line equation, namely $m(X + 1)$.
2. We would see $X^2 + (m(X + 1))^2 = 1$, which, after we expand terms becomes $(1 + m^2)X^2 + (2m^2)X + (m^2 - 1) = 0$.
3. This can be factored as: $(X + 1)((1 + m^2)X + (m^2 - 1)) = 0$. Therefore we find our two solutions: Either $X + 1 = 0$ or $(1 + m^2)X + (m^2 - 1) = 0$. The first equation gives us $X = -1$, which is our original point of intersection, $(-1, 0)$. The second equation gives us the other point of intersection, $X = (1 - m^2)/(1 + m^2)$.
4. If we insert this value back in to the line equation $Y = m(X + 1)$, we can solve for Y and find that $Y = 2m/(1 + m^2)$.
5. Thus given any slope m, we found the two points of intersection of the line and the circle. One point is the known point $(-1, 0)$ and the other point is the more exotic

$((1 - m^2)/(1 + m^2), 2m/(1 + m^2))$. Notice how this last point varies as we change m.

C. The study of algebraic geometry.

1. In this previous exercise, notice how we first used geometry to visualize the circle and lines and their two points of intersection and then applied algebra to find those precise points by using the equations that described the graphs.
2. This powerful synergy between geometry and algebra is the basis for the important field of study known as algebraic geometry.
3. In fact, as we will see in the next lecture, the points of intersection of lines and curves play a central role.

IV. A modern geometric approach to the Pythagorean triples.

A. A connection between slopes and points on the circle.

1. We now see that given any slope m, we can find that second point of intersection of the unit circle and the given line.
2. Suppose now that we select natural numbers a and b with a larger than b. If we consider the line having slope $m = b/a$, then we can quickly find the second point of intersection with the circle: $((1 - m^2)/(1 + m^2), 2m/(1 + m^2)) = ((1 - (b/a)^2)/(1 + (b/a)^2), 2(b/a)/(1 + (b/a)^2))$, which simplifies to $((a^2 - b^2)/(a^2 + b^2), (2ab)/(a^2 + b^2))$.

B. Discovering all Pythagorean triples.

1. Since this complicated point is on the unit circle, that implies we have a Pythagorean triple, namely, $(a^2 - b^2, 2ab, a^2 + b^2)$, which is exactly the formula we found for generating Pythagorean triples in the previous lecture.
2. However, now we know that we have found *all* Pythagorean triples because every triple corresponds to a point of intersection with the unit circle and one of our lines.
3. Thus this combination of algebra and geometry allowed us to prove that we have found *every* Pythagorean triple.

C. Conic sections and quadratics.

1. The circle is a special curve that is an example of what is called a conic section.
2. A conic section is any curve that can be realized by slicing an ice-cream-like cone with a plane.

3. Other conic sections are ellipses, parabolas, and hyperbolas. Their corresponding equations are all quadratic—they have exponents equal to 2.
4. Thus if we intersect any of these curves with a straight line, we will again have exactly two points of intersection.
5. In the next lecture we consider equations that are more complicated: They have an exponent of 3, and their graphs cannot be generated by simply slicing an ice-cream cone with a plane.
6. The subtle curves we are about to study will move number theory forward. These objects are known as elliptic curves.

Questions to Consider:

1. Consider the line with equation $y = (1/2)(x + 1)$. Verify that $(-1, 0)$ is a point on the line and on the unit circle $x^2 + y^2 = 1$. Find the second point of intersection of this line and the unit circle.
2. Verify that the point $(8/17, 15/17)$ is on the unit circle $x^2 + y^2 = 1$. Find the Pythagorean triple that corresponds to this rational point.

Lecture Eighteen

The Complex Structure of Elliptic Curves

Scope: An elliptic curve is a very delicate and important object that subtly twists through the plane. The gentle turns that grace these curves arise from the cubic Diophantine equations that describe them. We will extend the ideas we developed in the previous lecture to find rational points on a circle by studying intersections with certain lines, and we will see that the rational points on elliptic curves enjoy an incredibly rich arithmetic and geometric structure. This structure, which again involves studying the intersection of the curves and lines, is now understood through some very recent, remarkable 20th-century advances due to Louis Mordell and Barry Mazur. We will describe these results and mention a few open questions that continue to intrigue number theorists around the world. We will also see how these elliptic curves are, in actuality, level curves of a three-dimensional surface. Just as we might study topographic maps to understand the terrain on the surface of the earth, here we will examine these elliptic curves and realize that they can be viewed as slices of the surface of a doughnut. This delicious insight leads to many important theorems and conjectures. We will close this lecture by turning to some significant applications of these results, including the dramatic conclusion of Fermat's Last Theorem.

Outline

I. Elliptic curves and their images.
   A. Moving beyond quadratics and circles.
      1. In the previous two lectures we have focused on the Pythagorean equation, which involves exponents of 2 and thus is considered a quadratic equation.
      2. In the previous lecture we exploited the insight that natural-number solutions to the Pythagorean equation correspond to rational points on the unit circle.
      3. Here we take the insights we developed and apply them to more complex objects.

B. More subtle equations and curves.

1. Here we will study certain Diophantine equations that contain exponents 2 *and* 3. The equations we will consider all have the general form $y^2 = x^3 + ax + b$, for fixed given integers a and b.
2. These equations describe curves that can be graphed in the coordinate plane—just as we graphed the unit circle and other conic sections. The associated curves are called elliptic curves. For example, $y^2 = x^3 - x$ and $y^2 = x^3 - x + 1$ both represent elliptic curves.

C. A brief history of elliptic curves.

1. Returning again to the circle, we recall that if we wish to determine the length of the circle (its perimeter, better known as its circumference), then we can apply the ancient famous formula: Circumference = $2\pi r$, where r represents the radius of the circle.
2. The length of a curve is known as *arc length*. So the formula for the arc length of a circle is well-known.
3. It is much more difficult to compute the arc length of ellipses. Those computations involve complicated objects known as elliptic integrals. Associated with these elliptic integrals are functions later known as elliptic functions. These functions are connected with equations of the form $y^2 = x^3 + ax + b$, and thus these are now known as *elliptic curves*.
4. The study of elliptic curves began in the 19th century, and foundational progress was made by Norwegian mathematician Niels Abel and German mathematicians Carl Jacobi and Karl Weierstrass, along with Gauss and Legendre.

II. The arithmetic of elliptic curves.

A. Rational points on elliptic curves.

1. If x and y are two rational numbers that satisfy the equation for an elliptic curve, then the point (x, y) would be a point on the graph of that elliptic curve.
2. Just as with our exploration into the unit circle, here we wish to find rational points on elliptic curves—that is, rational values for x and y that satisfy the equation for the elliptic curve.

B. Connecting the dots with lines.

1. Since the highest exponent in the equation for an elliptic curve is 3, we call it a cubic.
2. Also because the highest power is 3, if we intersect its elliptic curve with any straight line having some slope m, then there will be up to three points of intersection.
3. For example, let us consider the intersection of the elliptic curve $y^2 = x^3 - x$ with the line $y = x$, the diagonal line that passes through the origin.
4. If we solve these equations simultaneously, we see $x^2 = x^3 - x$, which gives $x^3 - x^2 - x = 0$. If we factor out the x, this equation becomes $x(x^2 - x - 1) = 0$.
5. Solving this equation we see that either $x = 0$ or $x^2 - x - 1 = 0$. However we have already found the solutions to the second equation: $x = (1 \pm \sqrt{5})/2$, namely the golden ratio and its conjugate.
6. Finding the y values in this case is easy since they are all on the line $x = y$. That is, the x and y values are equal. So we found three points of intersection.

C. Focusing in on rational solutions to cubic equations.

1. It is a theorem from high school algebra that if a cubic equation having integer coefficients has two of its solutions equal to rational numbers then its third solution must also be a rational number.
2. To illustrate this fact, let us consider the cubic equation $x^3 - 4x = 0$. We notice that two of its solutions are rational, namely $x = 0$ and $x = 2$. Therefore the third solution must be rational, and indeed it is: $x = -2$. We can also see these solutions by factoring the equation: $x^3 - 4x = x(x - 2)(x + 2) = 0$.
3. This theorem holds an extremely important implication within the world of elliptic curves.
4. Suppose that we find two different rational points on an elliptic curve. If we connect those points with a straight line, then the line will intersect the elliptic curve at a third point (since the equation is a cubic). The theorem we just mentioned implies that the third point of intersection must also be a rational point.

5. So if we have two rational points on an elliptic curve, we can generate a third rational point: Simply connect those two points with a straight line, and the third point of intersection must be another rational point!

D. The rational points on an elliptic curve enjoy rich arithmetic structure.

1. We now notice that if we look at the graph of any elliptic curve, if we reflect that image over the horizontal x-axis, then it lands back onto itself. Namely, if we look through the x-axis, we see the mirror image of the curve above and below that axis. We say that the curve is "symmetric about the x-axis."
2. Moreover, if (x, y) is a rational point on an elliptic curve, then its reflection $(x, -y)$ is also a rational point on the elliptic curve.
3. We can pull all our observations together and discover that the rational points on an elliptic curve can be combined with a new type of arithmetic—one in which we can "add" two rational points on an elliptic curve to yield another rational point. We call this operation "addition," but it is not at all connected with usual addition of numbers.
4. Suppose that we wish to "add" two rational points on an elliptic curve. We first connect them with a straight line and look at the third point of intersection of this line and the curve. We now know that this third point of intersection will be another rational point on the elliptic curve. We consider that point's reflection over the horizontal axis. This gives us yet another rational point on the elliptic curve, and this point is defined to be the "sum" of the first two rational points.
5. So this "addition" is defined geometrically by studying the intersection of a line and a curve. We call it "addition" because under this operation, the rational points on an elliptic curve enjoy all of the basic properties that the integers enjoy under usual addition: The operation is associative, there is an identity element (that is, a version of 0), and every point has an additive inverse.
6. A collection of objects that has an operation that satisfies all these properties is called a *group* and is an abstract algebraic

structure. The area of abstract algebra known as *group theory* has its focus on identifying the different types of groups.

7. So the rational points on an elliptic curve form a group under this unusual "addition."
8. In 1921, British mathematician Louis Mordell was able to classify what types of groups these rational points could be. His result shows, among many other deeper consequences, that all the points on an elliptic curve (whether there are finitely many or infinitely many) can be found by successive "additions" of only *finitely* many rational points. Such groups are called *finitely generated* groups.
9. In 1977, Barry Mazur from Harvard University proved an amazing theorem that in some sense quantifies Mordell's theorem. Among other things, Mazur showed that if an elliptic curve had only *finitely* many rational points, then it can have no more than 16 of them.

III. From level curves to surfaces.

A. A topographical view of curves.

1. Let us return to the circle and ask, What if the circle was a slice of a simple three-dimensional surface. Could we visualize such a surface?
2. Certainly a sphere would be such a surface.
3. Let us now consider elliptic curves—for example, $y^2 = x^3 - x$. Notice that as the curve moves to the right, the top wing is rising up to infinity while the bottom wing is falling down to negative infinity. To view this curve more accurately, we must pretend that as those wings are heading in opposite directions, they are actually approaching each other. In fact, these two wings would actually meet—as if they were traveling on the surface of a ball. This is known as *stereographic projection.*
4. Thus we would now be looking at two closed loops as the elliptic curve. This is the level curve of some geometric object.
5. In this case, it is the level curve of the surface of a doughnut, which in mathematics is called a *torus*.
6. Notice that the circle comes from a 2^{nd}-degree equation and represents a slice of a sphere (an object with no holes), while

the elliptic curve comes from a 3rd-degree equation and represents a slice of a doughnut (an object with one hole).

B. Level curves and the genus of a surface.

1. The graph of a corresponding 4th-degree equation could be viewed as a slice of a three-holed doughnut. And in general, the higher degree an equation has, the more holes its associated surface has.
2. We saw in the previous lecture that the unit circle contains infinitely many rational points—that is a level curve of a zero-holed sphere.
3. Here we noted that some elliptic curves have infinitely many rational points while others have only finitely many rational points; these all represent a slice of a one-holed doughnut.
4. Mordell, in 1923, conjectured that for all curves that represent slices of surfaces having more than one hole (such as a three-holed doughnut), those curves contain only *finitely* many rational points.
5. In 1983, German mathematician Gerd Faltings proved Mordell's conjecture. Three years later, Faltings was awarded the Fields Medal for his groundbreaking work.
6. So elliptic curves—those special curves of degree 3—are the most enigmatic curves. If we have a smaller degree we know that we have infinitely many rational points; if we have a larger degree we know that we have only finitely many rational points. But elliptic curves can have either.

IV. The dramatic conclusion of Fermat's Last Theorem.

A. A proof by contradiction and the Frey curve.

1. Hidden within this delicate structure of elliptic curves was the solution to Fermat's Last Theorem.
2. In the late 1960s, French mathematician Yves Hellegouarch had an interesting idea. He assumed that for some odd prime number p there was a natural-number solution to the equation $a^p + b^p = c^p$. He then used these numbers to create the elliptic curve $y^2 = x(x - a^p)(x - b^p)$.
3. This elliptic curve would possess some very unusual properties owing to the fact that the sum of the numbers a^p and b^p is a perfect power of p.

4. Years later, German mathematician Gerhard Frey believed that such an elliptic curve would be so unusual that it would contradict an important conjecture about elliptic curves known as the Taniyama-Shimura-Weil conjecture.
5. In 1986, Kenneth Ribet of UC Berkeley proved that the truth of a special case of the Taniyama-Shimura-Weil conjecture would contradict the assumption that there was a natural-number solution to Fermat's equation. That is, Ribet proved that if a special case of the Taniyama-Shimura-Weil conjecture held, then that would imply the truth of Fermat's Last Theorem.

B. Andrew Wiles and his childhood quest.

1. Andrew Wiles is a British mathematician who as a young boy read the mathematical story of Fermat's Last Theorem. It was his childhood goal to find a proof.
2. Thus once he heard of Ribet's important result, Wiles decided to work full-time on proving the special case of the Taniyama-Shimura-Weil conjecture. He worked in total secrecy for seven years.
3. Finally, in June of 1993, at a conference held at the Isaac Newton Institute for Mathematical Sciences in England, he delivered a series of three lectures culminating with a proof of the Taniyama-Shimura-Weil conjecture and thus producing a proof of Fermat's Last Theorem.
4. During the peer-reviewing process, an error was uncovered. However, in September of 1994, a complete and correct proof was in hand, and Wiles fulfilled his childhood dream.

V. The larger study of algebraic geometry and its applications.

A. Today algebraic geometers continue to uncover new findings about elliptic curves. There are many open questions that remain—questions that generalize Fermat's Last Theorem in a variety of different directions. One such open question is known as the "abc conjecture."

B. The arithmetic of rational points on elliptic curves has implications within the context of factoring large numbers into primes. Thus the arithmetic of elliptic curves has implications into the modern practical world of cryptography.

Questions to Consider:

1. Consider the elliptic curve $y^2 = x^3 - x + 1$. Verify that the points (1, 1) and (0, 1) are both points on this curve.
2. Consider the elliptic curve $y^2 = x^3 - 4x$. What are the values of x for which $y = 0$? Does your answer lead to three rational points on the curve? (It is interesting to note that the three rational points you find are the only rational points on this curve. That is, there are only three rational solutions to this Diophantine equation!)

Lecture Nineteen
The Abundance of Irrational Numbers

Scope: Our focus up to this point has been primarily on the study of natural numbers and their ratios—the rational numbers. If we view these numbers as the *yin* of number theory, here in the remaining lectures we study the *yang*—the more enigmatic irrational numbers. These numbers, perhaps first discovered by the Pythagoreans, ran so counter to the original notion of number that many refused to accept them as actual numbers. Once humankind embraced these objects as numbers, the desire to understand their mysterious nature gave birth to an entirely new, uncharted branch of number theory. Here we will introduce the concept of irrationality, its early history, and some important examples—including π, e, and the more mysterious γ. After a brief review of decimal expansions of real numbers, we will discover that the irrational numbers are precisely those decimal expansions whose endless screed of digits never settles down and becomes periodic. This insight follows from the division algorithm we studied earlier, together with the so-called Pigeonhole Principle. While these numbers first appeared as strange and exotic to our ancient ancestors, we will discover that these irrational numbers, in fact, totally dominate the number theory landscape.

Outline

I. The Pythagoreans and the square root of 2.
   A. A Pythagorean view of number.
      1. The Pythagoreans viewed the natural numbers as the "God-given" numbers.
      2. They believed that one way to attain a closer relationship with the gods was through a deep understanding of the nuance of the "God-given" numbers—the natural numbers.
      3. They also explored the ratios of natural numbers but considered these more as a combination of two numbers rather than numbers in their own right.
      4. The Pythagoreans believed that all lengths could be measured using either natural numbers or ratios of natural numbers. This

belief is connected with the idea of commensurability, in which the ratio of the lengths of two objects equals a rational number.

B. A disturbing diagonal length.

1. If we adopt, for the moment, a Pythagorean mind-set regarding lengths, then we will run into trouble when we consider the length of a diagonal of a unit square.
2. Let us consider a square having side lengths equal to 1 unit.
3. If we draw a diagonal, then we can see that the length of this diagonal is larger than 1 and smaller than 2. Thus it cannot be a natural number.
4. Assuming the Pythagorean belief, we must conclude that this length is a ratio of natural numbers; that is, it must be a rational number, say a/b, for some natural numbers a and b. We will now see that this assumption will lead us to an impossibility.
5. Applying the Pythagorean Theorem to the right triangle formed, we discover that $(a/b)^2 = 1^2 + 1^2 = 2$. Thus in modern notation we note that $a/b = \sqrt{2}$; however, returning to the original equation we conclude that $a^2 = 2b^2$.
6. Factoring these identical numbers into primes reveals something disturbing. On the one hand, the number of factors of 2 in the factorization of a^2 is even while the number of factors of 2 in the factorization of $2b^2$ is odd. This contradicts the fundamental theorem of arithmetic that asserts the factorization into primes is unique.
7. This contradiction reveals a logical fallacy. Thus the Pythagorean assumption that all lengths are rational must be false. That is, we just proved that $\sqrt{2}$ is an *irrational number*—a number that is *not* a ratio of natural numbers.

C. The existence of irrational numbers.

1. Thus we discover that there are numbers that are not ratios of integers.
2. The Pythagoreans did not view these strange lengths as numbers but did acknowledge that such strange lengths—even if they were not "God-given" numbers—did exist.

3. It took hundreds (if not thousands) of years for people to retrain their intuition about number so as to embrace these irrational numbers as genuine numbers the way we do today.
4. We could adapt our argument showing that $\sqrt{2}$ is irrational to prove that both φ, which equals $(1 + \sqrt{5})/2$, and τ, which equals $(1 - \sqrt{5})/2$, are irrational. Thus we see that the golden ratio is another example of an irrational number. Moreover, if we return to the Binet formula for the n^{th} Fibonacci number that we derived in Lecture Six, $F_n = (\varphi^n - \tau^n)/\sqrt{5}$, we can be even more impressed by the amazing synergy between these irrational numbers. They can be combined in such a simple way and produce a natural number.

II. The irrationality of log 2.

A. The meaning of a logarithm.

1. To discover another important example of an irrational number, we return to the idea of a logarithm.
2. If we write $\log A = B$, then we mean that $10^B = A$. For example, $\log 100 = 2$ because $10^2 = 100$.

B. Another irrationality proof.

1. We now claim that log 2 is an irrational number.
2. To establish this claim, let us call this number B; that is, $\log 2 = B$. We now prove this assertion by contradiction, so we assume—contrary to what we hope to show—that B is a rational number, say $B = r/s$, for some natural numbers r and s.
3. Given that $\log 2 = B$, we know from the definition of log that $10^B = 2$. In view of our assumption, we see that $10^{r/s} = 2$, which is equivalent to $10^r = 2^s$. However, this equality is again impossible in view of the fundamental theorem of arithmetic: The prime factors on the right-hand side consist solely of 2s, while on the left-hand side we see both the primes 2 and 5 appearing.
4. The same number cannot be factored in two different ways, and thus we arrive at a contradiction—a logical fallacy. Hence our assumption must be false; that is, log 2 must in fact be an irrational number.

III. Decimal expansions of real numbers.

A. A brief review of real numbers and the real number line.

1. Just as we saw in Lecture Five with the golden ratio, both $\sqrt{2}$ and log 2 can be expressed as decimal numbers. A calculator can reveal the first few digits: $\sqrt{2} = 1.41421356\ldots$, and $\log 2 = 0.301029996\ldots$.
2. Numbers that have a decimal expansion are called *real numbers* and can be viewed as points on a number line.
3. Thus the real numbers can be viewed, informally, as all possible lengths of objects, together with their negatives and zero.

B. Decimal expansions and the rational numbers.

1. It is a straightforward task to find the decimal expansion of a rational number: We merely "long divide." Said in the language of number theory, we repeatedly apply the division algorithm.
2. If we consider the rational number 1/7 and perform the long division, then keeping track of the remainders we produce, we would see 1, 3, 2, 6, 4, 5, and then we would return to 1. These remainders must eventually repeat since there are only 7 possible values for the remainder when dividing by 7.
3. The fact that we must return to a previously seen remainder is an illustration of the Pigeonhole Principle.
4. Given this repeating-remainder phenomenon, we see that the decimal expansion must eventually become periodic.
5. This argument holds for the decimal expansion for any rational number. Thus every rational number has a decimal expansion that eventually becomes periodic.
6. The converse is also true: If a decimal expansion for a real number is eventually periodic, then it must be a fraction—a ratio of two integers.
7. For example, if we consider 0.6666..., then we see that it equals the rational number 2/3.

C. Irrational decimal expansions.

1. From the above analysis we conclude that a real number is a rational number if and only if its decimal expansion is eventually periodic.
2. If we stand this result on its head, we discover that a real number is irrational if and only if its decimal expansion is *never* eventually periodic. That is, its decimal expansion never repeats indefinitely.

3. Thus we can now immediately conclude that the decimal expansions for the golden ratio, $\sqrt{2}$, and log 2 will never become periodic.
4. We can generate other irrational numbers in terms of their decimal expansions. For example, the number 0.1010010001000010000010 0... is an irrational number.
5. Thus the decimal expansion provides us with a "modern" means of demonstrating that irrational numbers do exist.

IV. Almost all numbers are irrational.

A. Nonrepeating decimal numbers.

1. We have seen that nonrepeating decimal numbers are precisely the irrational numbers, and the decimal numbers that eventually become periodic are the rational ones.
2. We are more familiar with rational numbers, and thus the irrational numbers appear to us as exotic and exceptional. But are they, in reality?

B. Picking a number "at random."

1. If we were to pick a decimal number at random, what are the chances that it would be a rational number?
2. We can pick a decimal number "at random" by randomly generating its digits. We could roll a fair 10-sided die to generate the digits of the decimal expansion. If we rolled this die forever, the probability that the digits would become periodic and repeat forever is 0.
3. Thus, mathematically, the probability that a random decimal number is rational equals 0%, and the probability that a random decimal number is irrational equals 100%.

C. The rational numbers are rare.

1. This mathematical reality forces us to retrain our intuition and view of nature. In reality, the familiar rational numbers are the exception and the exotic irrational numbers are the norm.
2. This surprising realization is a wonderful opportunity to celebrate the power of number theory.

V. The famous numbers π and e.

A. The ancient constant π.

1. The number π is an ancient constant that is defined to be equal to the ratio of the circumference of a circle to its diameter.

2. Numerically, we can compute $\pi = 3.14159265\ldots$.
3. The number π is a very complicated number, and thus there are no "easy" ways of expressing it. There are many complicated ways, including as the famous infinite series $\pi = 4 - 4/3 + 4/5 - 4/7 + 4/9 - 4/11 + \cdots$.
4. To establish that this infinite series equals π requires techniques from calculus that we will not describe here.
5. The richness of π can also be seen by the fact that π is an irrational number. This technically complicated result follows the same logical reasoning as our previous irrationality proofs: We assume that π is rational and deduce a contradiction.

B. The modern constant *e*.

1. The number *e*, known as Euler's constant, is a number that helps us understand growth and change.
2. It is one of the most important numbers from calculus. Numerically, it is given by $e = 2.7182818284\ldots$.
3. The number *e* can also be expressed as an infinite series:

$$e = 1 + 1/2 + 1/(3 \times 2) + 1/(4 \times 3 \times 2) + 1/(5 \times 4 \times 3 \times 2) + \cdots .$$

4. Using this infinite series, it can be shown that *e* is also an irrational number.

C. The more mysterious constants from number theory.

1. In our discussion of prime numbers we came upon the Riemann zeta function, $\zeta(s) = 1 + 1/2^s + 1/3^s + 1/4^s + 1/5^s + \cdots$.
2. This function played a key role in the prime number theorem and is the centerpiece for the Riemann Hypothesis—one of the most important open questions in all of mathematics.
3. We saw in our discussion of square-free natural numbers from Lecture Eight the number $\zeta(2) = 1 + 1/2^2 + 1/3^2 + 1/4^2 + 1/5^2 + \cdots$, which we asserted equals $\pi^2/6$. This number also is known to be irrational.
4. What about $\zeta(3) = 1 + 1/2^3 + 1/3^3 + 1/4^3 + 1/5^3 + \cdots$? While there is no known "nice" closed form for this number as we have for $\zeta(2)$, we do know something about its value. In 1977, French mathematician Roger Apery proved that this number is, in fact, irrational. This series is now known as *Apery's number*.

5. Finally, we recall that the harmonic series from Lecture Eight given by $1 + 1/2 + 1/3 + 1/4 + 1/5 + \cdots$ diverged to infinity. In fact it grows very slowly, at the same rate as the natural logarithm, $\ln(n)$, that we saw in Lecture Nine.
6. More precisely, if we consider the difference $(1 + 1/2 + 1/3 + \cdots + 1/n) - \ln(n)$, then as *n* gets larger and larger, this difference approaches a number. This number is denoted by γ.
7. The first digits of the decimal expansion of γ can be given. It is known that $\gamma = 0.577215664\ldots$. However, no one has been able to prove that this number is irrational. This remains a very difficult open question. David Hilbert said that proving the irrationality of γ appears to be totally unattainable. It is said that G. H. Hardy offered to give up his prestigious chair at Oxford to anyone who proved that γ is irrational.
8. It is known that if γ is a rational number, say a/b, then *b* must be much greater than $10^{240,000}$. Open questions abound in the theory of irrationality.

Questions to Consider:

1. In this lecture we proved that $\sqrt{2}$ is irrational. Use a similar method to establish that $\sqrt{3}$ is also irrational. (At some point in your argument, consider the number of occurrences of the prime factor 3 on both sides of an equality.)
2. Suppose we are given an irrational number α. Verify that 10α (10 times α) is also irrational.

Lecture Twenty
Transcending the Algebraic Numbers

Scope: In the previous lecture, we discovered that almost all numbers are irrational numbers. Despite this reality, here we will show that the very sparse collection of rational numbers is spread all over the real number line—said mathematically, the rational numbers form a dense subset within the collection of real numbers. When we generalize the collection of rational numbers, we arrive at the world of algebraic numbers. This collection of numbers possesses a rich arithmetic structure that resembles the structure possessed by the rational numbers. We will then transcend the algebraic numbers and wonder if there are numbers that are not algebraic. These enigmatic numbers, called *transcendental numbers*, were not even known to exist. Joseph Liouville, in 1844, discovered a remarkable theorem connecting rational and algebraic numbers. His result offered the first mathematical proof that transcendental numbers do indeed exist. As background, we will return to the simpler issue of irrationality and discover the corresponding result in that context. We will then be ready to appreciate Liouville's remarkable result that launched an entire field known today as *transcendental number theory*, and we will highlight lingering open questions in this relatively new field of study.

Outline

I. The rationals within the reals.
  A. Decimal expansions of real numbers.
    1. We recall from the last lecture that the rational numbers are precisely those real numbers with decimal expansions that eventually become periodic.
    2. The irrational real numbers, therefore, are precisely those values having nonrepeating decimal expansions.
    3. Using this fact, we concluded that, in some sense that can be made mathematically precise, there are *more* irrational numbers than rational ones.

  B. Approximating an irrational number by rational numbers.
    1. Despite this dearth of rational numbers, we now discover that each irrational number can be approximated—as close as we wish—by the less common rational numbers.
    2. Truncating the decimal expansion of an irrational number offers us a rational approximation.
    3. So we are able to get as close as we wish to any irrational number by a rational one.
  C. The rational numbers are dense in the reals.
    1. We can also approximate, as closely as we want, any rational number by a *different* rational number.
    2. Thus we conclude that given any two different real numbers x and y, we can always find a rational number in between them.
    3. This fact shows us that the rationals are spread throughout the real number line. We say that the rationals are "dense" in the real numbers.

II. Generalizing the rational numbers.
  A. Solving linear equations.
    1. We begin by noticing that any rational number—for example, 3/5—is a solution to a linear equation. In this case, $5x - 3 = 0$.
    2. Thus we can view the collection of rational numbers as the collection of all solutions to equations of the form $sx - r = 0$, in which r and s are any given integers ($s \neq 0$). In this case, the solution is r/s, a rational number.
  B. Polynomial equations.
    1. If we now consider slightly more complicated equations—those that involve x^2 terms, then we find equations such as $x^2 - 2 = 0$, which has solutions $\pm\sqrt{2}$; or $x^2 + 1 = 0$, which has solutions $\pm i$; or even $x^2 - x - 1 = 0$, which has solutions $(1 \pm \sqrt{5})/2$.
    2. More generally, any sum of x's raised to natural number powers that are multiplied by integers and added together and then set equal to 0 is called a polynomial equation with integer coefficients. These equations always have solutions, and the number of solutions is equal to the highest power we see appearing on the unknown x.
    3. In practice, it is extremely challenging to actually find those solutions even though we know those solutions do exist.

C. Algebraic numbers.

1. We define the set of algebraic numbers to be the collection of all numbers that are solutions to any polynomial equation having integer coefficients.
2. For example, $\sqrt{2}$, i, and the golden ratio are all examples of algebraic numbers. Since these numbers are solutions to quadratic equations (equations having the highest x power equal to 2), we say these are algebraic of *degree* 2. The number $\sqrt[3]{5}$ is algebraic of degree 3, since it is a solution to a cubic equation: $x^3 - 5 = 0$. In fact, we have already noted that every rational number is an example of an algebraic number—the rational numbers are algebraic of degree 1.
3. More exotic algebraic numbers can be created by combining integers with the operations of addition, subtraction, multiplication, division, exponentiation, and taking roots.
4. For example, $\sqrt[3]{(1 - \sqrt{71})/(\sqrt[5]{29} + 31)^8}$ is an algebraic number.

III. Transcendental numbers.

A. Do transcendental numbers exist?

1. Given that we can create such extremely complicated numbers, we now wonder if all numbers are algebraic numbers—that is, solutions to polynomial equations with integer coefficients.
2. This question parallels our earlier discussion about whether all numbers are rational. There we saw that in fact not all numbers are rational—irrational numbers exist!
3. Do nonalgebraic numbers exist? If a number is not algebraic, it is called *transcendental*. That is, a number is transcendental if it is *not* a solution to *any* polynomial equation having integer coefficients.
4. So the question we have arrived at is, do transcendental numbers exist?
5. For hundreds of years, people believed that π is an example of a transcendental number, but no one was able to prove it.
6. It is hard to prove a number is transcendental—it is defined by what it is *not*!
7. In fact, one of the greatest open questions in mathematics into the 19th century was, do transcendental numbers exist?

8. The answer was finally given by the great French mathematician Joseph Liouville in 1844, in a most elegant theorem.
9. To inspire Liouville's work, we momentarily leave the subtle dichotomy of algebraic versus transcendental numbers and return back to the somewhat simpler issue of rational versus irrational numbers.

B. What does it mean to be rational?

1. We recall that the rational numbers are dense within the real numbers. In particular, if we are given any fraction, say 2/3, we can find other rational numbers that are as close to the first as we wish.
2. However, we will now show that those rational numbers that are *extremely* close to the original fraction must have *enormous* denominators.
3. For example, let us suppose that we found a rational number p/q that is different from 2/3 but extremely close to 2/3—say, for example, $|2/3 - p/q| < 1/3{,}000{,}000$.
4. If we combine the fractions we see: $|(2q - 3p)/(3q)|$, and we see that $|2q - 3p| \geq 1$. So we conclude that $1/(3q) \leq |2/3 - p/q| < 1/3{,}000{,}000$, which implies that $3{,}000{,}000 < 3q$, or equivalently, $1{,}000{,}000 < q$. That is, the denominator must exceed 1,000,000.
5. This principle can be generalized to show that even though the rationals are dense in the real numbers, the fractions "repel" other rationals having small denominators. This result can be stated as the following theorem: Let r/s be a fixed fraction. Then there is a postive constant number c such that for every rational number p/q not equal to r/s, we have $c/q < |r/s - p/q|$.
6. To prove this theorem, we notice that since $p/q \neq r/s$, $(ps - rq)/(qs) \neq 0$. That is, $|ps - rq| \geq 1$. Thus we see that $1/sq < |r/s - p/q|$, or equivalently, $c/q < |r/s - p/q|$, where the constant $c = 1/s$. This establishes our result.

C. Discovering a number that "attracts" rationals.

1. Our theorem can be summarized as follows: If we have a rational number, then any other rational numbers that are very close to the first fraction must have a relatively large denominator.
2. Put on its head, we note that this result is equivalent to the following: If we have a number α that has an endless list of

rational numbers approaching it with relatively *small* denominators, then α *cannot* be a rational number; that is, α must be irrational.

3. For example, if we consider the number

   1.1001000010000001000000001000000000001000...,

   then we can find amazingly good rational approximations having relatively *small* denominators. For example, notice that 1.1 (which equals 11/10) is very close to our number—their difference is approximately 0.0001 (or 1/10,000). So with a denominator of just 10, we are nearly within 1/10,000 of our original number. Since we have infinitely many such amazing rational approximations relative to the size of their denominators, we can apply our theorem to conclude that the original number must be irrational.
4. Of course we can confirm that this number is indeed irrational since its decimal expansion is nonrepeating.
5. Our theorem can be extended to algebraic numbers, and this was the amazing insight of Liouville.

IV. Liouville's important theorem.

A. A subtle fact about algebraic numbers.

1. Liouville found a generalization of our result about rational numbers to algebraic numbers. Let α be an algebraic number having degree d. Liouville proved that there exists a positive constant c such that for all rational numbers $p/q \neq \alpha$, we have that $c/q^d < |\alpha - p/q|$.
2. This amazing result is now known as *Liouville's Theorem*. Notice that Liouville's Theorem agrees with our earlier result if $\alpha = r/s$ (in that case, the degree $d = 1$).
3. Just as we saw before, this result implies that if α is an algebraic number, then any rational number p/q that is relatively close to α must have a relatively large denominator q.
4. Equivalently, we see that *if* we find a number α that has an endless list of rational numbers approaching α at an amazingly fast rate compared to their relatively *small* denominators, then α *cannot* be algebraic; that is, α must be transcendental!

B. Amazing approximations to Liouville's number.

1. With his beautiful result in hand, Liouville considered the number L = 1.1100010000000000000000100000..., where the number of 0s between consecutive 1s grows dramatically according to a specified pattern.
2. This number has an endless list of rational numbers *incredibly* close to it that have relatively tiny denominators. For example, notice that the rational number 1.110001 (which equals 1,110,001/1,000,000) is within nearly $1/10^{24}$ of Liouville's number L.
3. We can apply Liouville's Theorem to conclude that these amazing rational approximations with relatively small denominators are too close to L to allow L to be an algebraic number—they contradict Liouville's Theorem about algebraic numbers. Hence, L must be transcendental! Transcendental numbers exist!
4. This was the first number shown to be transcendental, and it is now known as *Liouville's number*.

V. Life after Liouville.

A. Famous transcendental numbers.

1. Liouville found the first transcendental number in 1844. Nearly 30 years later, in 1873, French mathematician Charles Hermite proved that e is transcendental; and by 1882, German mathematician Ferdinand von Lindemann proved that π is transcendental.
2. The methods to prove these numbers are indeed transcendental are extremely complicated and technical. But they all have the same first step: Assume the number in question is algebraic and arrive at a contradiction—a logical fallacy.

B. The Gelfond-Schneider Theorem.

1. In David Hilbert's great address in 1900 stating the major open questions of mathematics, he asked if $2^{\sqrt{2}}$ is transcendental.
2. More generally, he asked: If we are given algebraic numbers α and β, such that α does not equal 0 or 1, and β is irrational, then is α^β always transcendental?

3. Much to many people's surprise, only 34 years later, this question was answered by the work of Russian mathematician Aleksandr Gelfond and German mathematician Theodor Schneider, who independently proved that such numbers are all transcendental.

C. Almost all numbers are transcendental.
   1. Just as we saw in the previous lecture that the irrational numbers dominate the world of numbers, here we note that it can be shown that the transcendental numbers are the norm.
   2. If we were to randomly pick a number, it is with 100% probability that we would pick a transcendental number and with probability 0% we would select an algebraic number.

D. Open questions remain.
   1. Despite the fact that "almost all" numbers are transcendental, many questions remain open.
   2. For example, are $e + \pi$ and $e\pi$ transcendental? Most number theorists believe so, but no one has a proof. In fact, no one can even prove that these numbers are irrational.

Questions to Consider:

1. Find a rational number that is a solution to $4x + 5 = 0$.
2. The number $1/\sqrt[3]{2}$ (the reciprocal of the cube root of 2) is algebraic. Find a polynomial equation having integer coefficients for which $1/\sqrt[3]{2}$ is a solution.

Lecture Twenty-One
Diophantine Approximation

Scope: Inspired by Joseph Liouville's foundational theorem from 1844, here we will consider the notion of "inexpensive" rational numbers—ratios whose denominators are relatively small. This theme naturally leads us to the question: How well can we approximate a real number by a rational number having a denominator that is relatively modest in size? The answer to this question was given by Johann Dirichlet in 1842, and in some sense, the seminal work of Dirichlet and Liouville gave birth to an area of study now known as *Diophantine approximation*. As we will see, Dirichlet's result also offers a new definition of irrational numbers that is equivalent to the standard one we studied earlier. We will also describe a deep 19th-century result of Leopold Kronecker on the multiples of irrational numbers. Kronecker's Theorem leads to a wide array of interesting consequences, including insights into the motion of billiard balls and planets, and why there is a power of 2 whose digits begin with your social security number.

Outline

I. A search for "inexpensive" rational numbers.
   A. Approximating real numbers by rationals.
      1. In Lecture Nineteen, we discovered that the rational numbers are dense on the real number line—meaning that we can find a rational number within any given small interval around any given real number.
      2. Truncating the decimal expansion of a real number is one possible way to generate a rational number that is extremely close to the given real number.
   B. "Inexpensive" rational numbers.
      1. In the previous lecture we saw that if we consider how close a rational approximates certain real numbers in terms of the size of the rational's denominator, then we might be able to make some additional conclusions.

2. Liouville's Theorem tells us that if we have an algebraic number α [alpha], then any rational number that is extremely close to α must have a relatively large denominator.
3. This result inspires us to view the rational numbers as having a "cost" determined by the size of their denominators. The larger the denominator, the greater the cost of the rational number.
4. A relatively "inexpensive" rational is one with a relatively small denominator. For example, 22/7 is "cheaper" than 31/10, since the first rational would "cost" only $7, while the second would cost $10.
5. This leads us to an interesting question: Suppose we have a fixed amount of money in the bank, say Q dollars, and we wish to buy a rational number that approximates a given real number α (mathematically termed α but sometimes called "A" by way of example). What is the best rational approximation to this number that we can afford? That is, how close can we get to the given α by rational numbers whose denominators are less than or equal to Q?
6. We can no longer use the fact that all the rational numbers are dense in the real numbers since the subcollection of rational numbers having denominators that do not exceed Q is no longer dense. In fact, we say this subcollection is *discrete*.
7. This subtle question of approximating numbers by rationals having denominators that are not too large launches us into an area of number theory known as *Diophantine approximation*.

C. Dirichlet's Theorem.
1. Johann Dirichlet, whom we studied earlier in our discussions of primes in arithmetic progressions, proved the first result in the area of Diophantine approximation in 1842.
2. Dirichlet's Theorem: Let α be a real number and $Q > 1$ be a natural number. Then there exists a rational number p/q such that $|\alpha - p/q| \leq 1/(Q + 1)q$, and also $1 \leq q \leq Q$.

3. The proof of Dirichlet's Theorem involves the Pigeonhole Principle that we applied several times throughout our course.

D. The idea of the proof of Dirichlet's Theorem.
1. To illustrate the idea of the proof, we consider a particular simple example. Suppose we wish to approximate π, and our Q equals 7. How do we find the rational p/q that Dirichlet's Theorem asserts exists?
2. First we cut up the interval from 0 to 1 into 8 equal subintervals (each having length 1/8). If we had 9 points in the interval from 0 to 1, then by the Pigeonhole Principle we would know that at least 2 of them would have a distance between them that would be less than or equal to 1/8.
3. Now we consider the following 9 numbers: 0, 1, and then the *fractional parts* of $1 \times \pi$, $2 \times \pi$, $3 \times \pi$, $4 \times \pi$, $5 \times \pi$, $6 \times \pi$, and $7 \times \pi$. These fractional parts can be computed as:

$$0 = 0.000000\ldots$$
$$\{1 \times \pi\} = 0.141592\ldots$$
$$\{2 \times \pi\} = 0.283185\ldots$$
$$\{3 \times \pi\} = 0.424777\ldots$$
$$\{4 \times \pi\} = 0.566370\ldots$$
$$\{5 \times \pi\} = 0.707963\ldots$$
$$\{6 \times \pi\} = 0.849555\ldots$$
$$\{7 \times \pi\} = 0.991148\ldots$$
$$1 = 1.000000\ldots .$$

4. At least 2 of these numbers must be within 1/8 (which equals 0.125) of each other. Amazingly, there are only 2 that are within this narrow difference: $\{7 \times \pi\}$ and 1. Since $7\pi = 21.991148\ldots$, we see that $|(7\pi - 21) - 1| \leq 1/8$; that is, $|7\pi - 22| \leq 1/8$. If we divide both sides by 7, we find that $|\pi - 22/7| \leq 1/(8 \times 7)$.
5. Since in this example we took $Q = 7$, we see that indeed we have $|\pi - 22/7| \leq 1/((Q + 1) \times 7)$ *and* $1 \leq 7 \leq Q$.
6. So we find that 22/7 is an extremely good approximation to π: It is within $1/(8 \times 7)$, which equals 0.01785..., of π.
7. This Pigeonhole Principle actually can be applied in general to prove the result for the real number α and the denominator bound Q.

II. A Diophantine definition of irrationality.

A. A property of irrational numbers.

1. We recall the statement of Dirichlet's Theorem: Let α be a real number and $Q > 1$ be a natural number. Then there exists a rational number p/q such that $|\alpha - p/q| \leq 1/(Q+1)q$, and also $1 \leq q \leq Q$.
2. If α is an irrational number, then as we let Q get larger and larger, we will find an infinite list of rationals p/q satisfying Dirichlet's inequality.
3. Because q is smaller than $Q + 1$, it follows that $1/(Q+1)q < 1/q^2$. Therefore we can weaken the inequality in Dirichlet's Theorem and conclude that there exists a rational number p/q satisfying $|\alpha - p/q| < 1/q^2$.
4. Thus if α is an irrational real number, then there exist infinitely many different rational numbers p/q that satisfy the inequality $|\alpha - p/q| < 1/q^2$.

B. A new definition for irrationality.

1. In fact, the converse of this result is also true: If α is a number such that there exist infinitely many different rational numbers p/q satisfying the inequality $|\alpha - p/q| < 1/q^2$, then α must be irrational.
2. This statement can be proven using our warm-up result in Lecture Twenty used to inspire Liouville's Theorem.
3. Thus we come upon a Diophantine approximation definition of irrationality: A real number α is irrational if and only if there exist infinitely many different rational numbers p/q satisfying the inequality $|\alpha - p/q| < 1/q^2$.
4. In many advanced applications, this definition is helpful.

III. Kronecker's Theorem on integer multiples of irrationals.

A. Integer multiples of irrational numbers.

1. The key idea in the proof of Dirichlet's Theorem was to consider the fractional parts of integer multiplies of α. We write $\{x\}$ for the *fractional part of x*—for example, $\{6.132\} = 0.132$ and $\{57.6\} = 0.6$.
2. In our example that illustrated Dirichlet's proof, we considered the first few integer multiples of the irrational number π and focused on their fractional parts. All those numbers must be within the range 0 to 1. If we return to those values, we again see:

$\{\pi\} = 0.141592\ldots$
$\{2\pi\} = 0.283185\ldots$
$\{3\pi\} = 0.424777\ldots$
$\{4\pi\} = 0.566370\ldots$
$\{5\pi\} = 0.707963\ldots$
$\{6\pi\} = 0.849555\ldots$
$\{7\pi\} = 0.991148\ldots$.

3. If we plot these points, we see that they are spread fairly evenly along the line segment from 0 to 1. In fact, if we consider the fractional parts of larger integer multiples of π, then we would see that those values begin to fill up more of the little gaps between the previous (smaller) multiples.
4. As we consider larger and larger integer multiples, those points appear to want to fill up the entire interval—in other words, if we pick any two points between 0 and 1, there will be some larger integer multiple of π whose fractional part is between these two points.

B. Kronecker's Theorem.

1. In fact, this observation is an example of a general principle about the fractional parts of the integer multiples of any irrational number. Those values will always be dense in the line segment between 0 and 1.
2. This result, first proved by German mathematician Leopold Kronecker in 1884, is now known as *Kronecker's Theorem*. It can be stated mathematically as the following theorem: Let α be an irrational real number. Then the infinite sequence $\{\alpha\}$, $\{2\alpha\}$, $\{3\alpha\}$, $\{4\alpha\}$, ... is dense in the interval between 0 to 1.

IV. Applications to billiards and the orbits of planets.

A. The trajectory of an idealized billiard ball.

1. Suppose we have a square frictionless billiard table with no pockets and an idealized ball that after it is placed into motion will remain in motion forever, bouncing off the sides of the table so that the angle at which the ball hits the side is equal to the angle of its trajectory off that wall.

2. As a consequence of Kronecker's Theorem, there are only two possibilities for the path the billiard ball makes: Either the path is periodic or the path is dense on the billiard table.
3. Why is this connected with Kronecker's Theorem? The path is periodic precisely when the initial slope of the path is rational and the path is dense precisely when the initial slope of the path is irrational.

B. The trajectory of planets.

1. Kronecker's result is an example of a mathematical proposition essentially implying that what is not impossible will eventually occur, no matter how improbable.
2. As another illustration, suppose that we have a group of planets revolving around the sun at different rates. If they all begin their orbits along the same line of sight from the sun, then Kronecker's result implies that even though the orbits will look totally out of phase, at some point they will all essentially be aligned.
3. We can see this phenomenon for ourselves with pairs of blinking lights.

C. Powers of 2 and you.

1. We return to a question we posed at the end of Lecture Two. Using Kronecker's Theorem it is possible to prove that given any natural number A, there exists a natural number B so that if we read off the left-most digits of the number 2^B, they will coincide with the given natural number A.
2. That is, given any run of digits, there exists a power of 2 that begins with that run. So there is a power of 2 that begins with your social security number.
3. How can we make this assertion believable? We first consider the logarithm of 2^B. By properties of logarithms, it follows that $\log(2^B) = B\log 2$, in other words, $\log(2^B)$ is actually an integer multiple of $\log 2$. We now recall from Lecture Nineteen that we proved that $\log 2$ is irrational.
4. Thus we can apply Kronecker's Theorem to conclude that the fractional parts of integer multiples of $\log 2$ are dense in the interval from 0 to 1. It is this density property that allows us to find the exponent B for which 2^B is "close" to the given list of digits in A.

Questions to Consider:

1. Using your arithmetic skills or a calculator, find the smallest power of 2 that begins with the digit 7.
2. Give as many reasons as you can for why 22/7 is a better approximation to π than 31/10.

Lecture Twenty-Two
Writing Real Numbers as Continued Fractions

Scope: Throughout this course we have expressed real numbers—that is, numbers that correspond to points on a number line—as endless decimal expansions. In this lecture we will ask, is there another systematic method of expressing real numbers? The answer is "yes": There exists an entirely different approach to real numbers—one that leads to expansions now known as *continued fractions*. Here we will study this algorithm for writing real numbers as a repeated fraction-within-fraction and explore its ancient history. By considering several illustrations, we will discover how this method of writing real numbers leads to new insights and reveals otherwise hidden structure within the real numbers. We will then revisit the golden ratio and discover that, in some strange sense, it is the "least irrational" of all the irrational numbers—thus adding another layer to its mystery and prominence.

Outline

I. Recalling an algorithm of Euclid's.

A. The Euclidean algorithm.

1. We recall from our divisibility discussions in Lecture Ten a desire to find the greatest common factor of two natural numbers.
2. Euclid, in his *Elements of Geometry*, developed an algorithm that offered an explicit procedure for finding the greatest common factor.
3. The basic method involves repeated applications of the "division algorithm": Given natural numbers a and b, there exists a unique quotient q and unique remainder r that satisfy $a = bq + r$ and $0 \leq r < b$.
4. The key point is that the remainder r is always smaller than the divisor b.

B. An illustrative example.

1. Let's find the greatest common factor of 41 and 130. These numbers are small enough that we can find their greatest common factor by simply factoring each number. We note that 41 is a prime and that $130 = 2 \times 5 \times 13$; thus the largest factor they have in common is 1. That is, 41 and 130 are relatively prime.
2. We will now find the greatest common factor of 41 and 130 by applying the Euclidean algorithm in order to illustrate the method. We systematically apply long division until we come upon a remainder of 0.
3. The Euclidean algorithm reveals:

$$130 = 3 \times 41 + 7$$
$$41 = 5 \times 7 + 6$$
$$7 = 1 \times 6 + 1$$
$$6 = 6 \times 1 + 0. \leftarrow \text{We see 0, so the process ends.}$$

4. The last *nonzero* remainder we see equals the greatest common factor. In this case we see 1, which is what we found by simply factoring.
5. This process will always end in a finite number of steps, as the remainders always shrink in size and are all natural numbers until we hit 0.

C. Writing a quotient as a fraction-within-fraction.

1. We now attempt to express the rational number 130/41. As a first step, we rewrite the first three equations we just found as:

$$130/41 = 3 + 7/41$$
$$41/7 = 5 + 6/7$$
$$7/6 = 1 + 1/6.$$

2. We suddenly see structure. Ratios and their reciprocals appear: 7/41 and then 41/7; 6/7 and then 7/6. In fact, 7/41 = 1/(41/7), and 6/7 = 1/(7/6).
3. Using these identities, we can substitute these equivalent values in our formula to deduce:

$$\begin{aligned} 130/41 &= 3 + 7/41 \\ &= 3 + 1/(41/7) \\ &= 3 + 1/(5 + 6/7) \\ &= 3 + 1/(5 + 1/(7/6)) \\ &= 3 + 1/(5 + 1/(1 + 1/6)). \end{aligned}$$

4. Thus we see that we can write 130/41 as $3 + 1/(5 + 1/(1 + 1/6))$.

5. This representation as a fraction within a fraction within a fraction is called a *continued fraction expansion.*
6. Eratosthenes and others expressed ratios as continued fractions.

D. Continued fractions of rational numbers.

1. Because we can perform the Euclidean algorithm with any two natural numbers, we see that we can write any ratio of natural numbers as a continued fraction of the generic form $a_0 + 1/(a_1 + 1/(a_2 + 1/(\ldots + 1/a_n)))$, where the a's are all natural numbers.
2. Moreover, since the Euclidean algorithm will always terminate in a finite number of steps, we see that all these continued fraction expansions will terminate as well; that is, there are only finitely many a's. In fact, upon further inspection we see that the a's are precisely the quotients we computed in our division process.
3. Similarly, it follows that any rational number whatsoever can be expressed as a finite continued fraction of the generic form $a_0 + 1/(a_1 + 1/(a_2 + 1/(\ldots + 1/a_n))\ldots)$, where the a_0 is an integer (it might be negative if the original rational number is negative) while all the other a's remain natural numbers.
4. It is also a straightforward task to show that any finite continued fraction must equal a rational number. For example, the continued fraction $2 + 1/(4 + 1/3) = 2 + 1/(13/3) = 2 + 3/13 = 29/13$.
5. Thus we have just proved that a number is a rational number if and only if it can be expressed as a finite continued fraction of the form $a_0 + 1/(a_1 + 1/(a_2 + 1/(\ldots + 1/a_n)))$, where the a_0 is some integer and all the other a's are natural numbers.
6. This fraction-within-fraction notation becomes very cumbersome, so we adopt some more compact notation. We write $[a_0, a_1, a_2, \ldots, a_n]$ for the continued fraction $a_0 + 1/(a_1 + 1/(a_2 + 1/(\ldots + 1/a_n)))$. So, for example, we could write $140/13 = [3, 5, 1, 6]$ and $29/13 = [2, 4, 3]$.

II. Writing real numbers as continued fractions.

A. A limitation to the Euclidean algorithm.

1. Given that the numbers appearing in the continued fraction expansion for a rational number are the successive quotients found in the Euclidean algorithm, in some sense, the continued fraction expansion holds all the information from the Euclidean algorithm.
2. Of course, the Euclidean algorithm requires two integers, and the continued fraction expansion equals the quotient, or ratio, of those two integers.
3. Furthermore, there is no way to apply the Euclidean algorithm with *irrational* numbers, and so we ask, is there a way of finding a continued fraction expansion for an irrational number?
4. Without any additional work, we can make one important observation: If an irrational number can be expressed as a continued fraction, then that continued fraction must never end, for we have shown that if a continued fraction terminates after finitely many steps, then it must equal a rational number.
5. Hence, *if* a continued fraction expansion can be constructed for an irrational number, it must have an endless fraction-within-fraction structure.

B. Strange successive reciprocals of decimals.

1. To discover how to find a continued fraction expansion for irrational numbers, we return back to our previous example, 130/41, and wonder if we can find its continued fraction expansion *without* explicitly applying the Euclidean algorithm.
2. Perhaps we could extend such an alternative procedure to find the continued fraction expansions for irrational numbers.
3. So we will view 130/41 now as a decimal: $130/41 = 3.1707317073\ldots$. We now remove the integer part and write the fractional part as 1 divided by the reciprocal of the fractional part: $130/41 = 3 + 1/(1/0.1707317073\ldots) = 3 + 1/(5.857142857142\ldots)$.
4. If we repeat this process we see:

$$\begin{aligned} &3 + 1/(5.857142857142\ldots) \\ &= 3 + 1/(5 + 1/(1/0.857142857142\ldots)) \\ &= 3 + 1/(5 + 1/(1.1666\ldots)) \\ &= 3 + 1/(5 + 1/(1 + 1/(1/0.1666\ldots))) \\ &= 3 + 1/(5 + 1/(1 + 1/6)). \end{aligned}$$

5. Thus, we rediscovered the continued fraction expansion we found earlier—but without using the Euclidean algorithm, using only the decimal expansion of 140/31.

C. A continued fraction algorithm for real irrational numbers.
   1. We will now extend the previous process to generate the continued fraction expansion to irrational numbers.
   2. We remove the integer part of the number and then consider 1 divided by the reciprocal of the fractional part and repeat this process.
   3. This method will generate a continued fraction for any real number—rational or irrational.

D. Two illustrations.
   1. Our method to find the continued fraction for any decimal number using a calculator is to first record the integer part of the number as a_0 and then subtract that part so that we are left with the fractional part. We then take the reciprocal of the fractional part and remove its integer part and call it a_1. We continue this process to generate all the terms in the continued fraction expansion.
   2. Let's compute the first number we proved was irrational: $\sqrt{2}$. We write the decimal expansion of

$$\begin{aligned}\sqrt{2} &= 1.414213\ldots \\ &= 1 + 0.414213\ldots \\ &= 1 + 1/2.414213\ldots \\ &= 1 + 1/(2 + 0.414213\ldots).\end{aligned}$$

   3. At this point we see a repetition in the fractional parts. When we take a reciprocal again, we will see an integer part equal to 2, and these numbers will repeat. Thus, just as we saw with decimal expansions of *rational* numbers, we see now that the continued fraction for the *irrational* number $\sqrt{2}$ is periodic: $\sqrt{2} = [1, 2, 2, 2, \ldots]$.
   4. If we now turn to the second number we established was irrational, log 2, then using a calculator and this procedure we would see:

$$\begin{aligned}\log 2 &= 0.301029995663981\ldots \\ &= 0 + 0.301029995663981\ldots \\ &= 0 + 1/3.32192809\ldots \\ &= 0 + 1/(3 + 0.32192809\ldots) \\ &= 0 + 1/(3 + 1/3.1062837\ldots) \\ &= 0 + 1/(3 + 1/(3 + 0.1062837\ldots)) \\ &= 0 + 1/(3 + 1/(3 + 1/9.408778\ldots)) \ldots .\end{aligned}$$

   5. Continuing in this manner, we would see that the continued fraction expansion for log 2 begins [0, 3, 3, 9, 2, 2, 4, 6, 2, 1, 1, 3, 1, 18, 1, 6, 1, 2, 1, ...].
   6. We note that here there is no obvious pattern to the natural numbers appearing in the continued fractions. Those natural numbers are called *partial quotients*, whether they form a pattern or not.
   7. With both of these irrational numbers, we see that their continued fraction expansions are indeed endless, as we predicted earlier.

III. A new way to identify irrational numbers.
   A. Terminating continued fractions. We recall that we showed that a number is a rational number if and only if its continued fraction expansion terminates in finitely many steps; that is, there are only finitely many partial quotients.
   B. Endless continued fractions.
      1. In view of this fact and the continued fraction algorithm we found for decimal numbers, we see that irrational numbers have unending continued fraction expansions.
      2. In fact, we see that a real number is an irrational number if and only if its continued fraction expansion is unending.
      3. Thus we come upon a new definition for irrationality—one that is equivalent to the standard one but nonetheless has a very different quality.
      4. So the theory of continued fractions allows us to look at the notion of irrationality in an entirely new light.

IV. Famous numbers and their continued fractions.
   A. Another way to write π.
      1. If we compute the continued fraction for π, then we would see:

$$\begin{aligned}\pi &= 3.141592654\ldots \\ &= 3 + 0.141592654\ldots \\ &= 3 + 1/7.06251328\ldots \\ &= 3 + 1/(7 + 0.06251328\ldots) \\ &= 3 + 1/(7 + 1/15.99659\ldots).\end{aligned}$$

      2. If we continued this process, we would see $\pi = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 3, \ldots]$.

3. There appears to be no pattern to the partial quotients, and we will say a bit more about this in the next lecture.
4. The theory of continued fractions was used by von Lindemann in 1882 to prove that π is transcendental.
5. If we look at the first two terms in the continued fraction expansion and ignore the rest, we notice that $3 + 1/7 = 22/7$, the familiar rational approximation for π. This observation will be expanded on in the next lecture.

B. Another way to write *e*.

1. The continued fraction expansion for π appeared to have no easy-to-identify pattern. Let us now consider the continued fraction expansion for *e*.
2. If we begin with the decimal $e = 2.718281828459045235\ldots$, then we find that $e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12, \ldots]$. It can be proven this pattern continues: 1, 1, and then the next even number.
3. This incredible structure within *e* only comes into focus through its continued fraction expansion.
4. Given this predictable progression, we see that the continued fraction expansion for *e* is endless. Hence we see that *e* must indeed be irrational.

V. The golden ratio and Fibonacci numbers, revisited.

A. The "least irrational" irrational number.

1. If a real number has a finite continued fraction expansion then it is a rational number, and otherwise it is irrational.
2. In some sense, large partial quotients in a continued fraction for a number α give rise to rational approximations to α that are extremely close to α relative to the size of the denominators of the rational approximants.
3. Recalling from Lecture Twenty that the rational numbers themselves have no good rational approximations with relatively small denominators, we see that in some informal sense the larger the partial quotients, the "more irrational" a number is; the smaller the partial quotients, the "less irrational" a number is.
4. Liouville's number is transcendental because it has such amazing rational approximations by rationals having relatively small denominators. Therefore Liouville's number must have some incredibly enormous partial quotients in its continued fraction expansion.
5. Transcendental numbers are as far as possible from being rational.
6. So what would be the "least irrational" number? Since it must be irrational, we know that its continued fraction expansion must never end. We also know that the smaller the partial quotients, the "less irrational" the number is. The smallest partial quotient possible would be the smallest natural number, which of course is 1. Thus in some informal sense, the "least irrational" irrational number has a continued fraction expansion equal to $[1, 1, 1, 1, 1, \ldots] = 1 + 1/(1 + 1/(1 + 1/(1 + 1/(1 + \ldots))))$.
7. But in Lecture Six, we proved that this continued fraction equals the golden ratio.
8. So the famous golden ratio is, in some sense, the "least irrational" irrational number! Another title it can possess with pride.

B. Truncating the infinite continued fraction.

1. In the next lecture we will ask, What if we were to truncate the continued fraction expansion for the golden ratio?
2. Then we would have a continued fraction expansion that is finite in length and of the form $[1, 1, 1, \ldots, 1]$.
3. Since these continued fraction expansions are finite, they must equal rational numbers. What are they? $[1] = 1/1$; $[1, 1] = 2/1$; $[1, 1, 1] = 3/2$; $[1, 1, 1, 1] = 5/3$; $[1, 1, 1, 1, 1] = 8/5$. We are uncovering ratios of consecutive Fibonacci numbers, a fact we proved for ourselves in Lecture Six.

Questions to Consider:

1. Use the Euclidean algorithm and the procedure outlined in the lecture to find the continued fraction expansion for 18/7.
2. Use a scientific calculator with a key for *e* (or "exp") to confirm that the continued fraction for *e* begins $[2, 1, 2, 1, 1, 4, 1, 1, 6, \ldots]$.

Lecture Twenty-Three
Applications Involving Continued Fractions

Scope: In this lecture we will describe how the continued fraction expansion of a number is connected with our earlier quest to find excellent rational approximations to real numbers. In fact, we will see how truncating the continued fraction of a real number produces the world's best rational approximations to that number. In particular, we will see that this algorithm generates the so-called *best rational approximants*. We will then return to the musical conundrum we considered in our discussion of geometric progressions at the opening of this course and use these ideas from Diophantine approximation to see why we have adopted a 12-note chromatic scale. We have seen earlier in this course that the decimal expansions for quadratic irrational real numbers will never become periodic, because these numbers are irrational. In this lecture we will discover some remarkable periodic patterns that only come into focus when we consider the continued fraction expansions of these quadratic irrationals. This structure can be exploited to find all natural-number solutions to the Pell equations that we studied in our sojourn into Diophantine equations. We will close with some famous vexing open questions involving continued fractions.

Outline

I. A search for the best rational approximants.

A. Dirichlet's Theorem, revisited.

1. Recall that Dirichlet's Theorem asserts that for any real number α and any natural number $Q > 1$, we can find a rational number p/q with $1 \le q \le Q$ that is relatively close to α; specifically we have that $|\alpha - p/q| \le 1/(Q+1)q$.

2. Throughout the previous two lectures we have been concerned with how well a rational approximates a real number α relative to the size of the denominator of the rational approximant.

3. One way to measure this delicate balance between denominator size and the quality of approximation to α is to multiply the denominator by the distance between the rational number and α. That is, we could study the quantity $q \times |\alpha - p/q|$, which equals the quantity $|\alpha q - p|$. In some sense, this quantity is a weighted measure of how well p/q approximates α.

4. By Dirichlet's result we see that the rational p/q appearing in his theorem satisfies $|\alpha q - p| \le 1/(Q+1)$. Notice that as Q gets larger, $1/(Q+1)$ gets smaller.

5. If we now assume that α is irrational, then as we let Q take on larger and larger values without bound, we can generate an endless list of rational numbers $p_1/q_1, p_2/q_2, p_3/q_3, \dots$, satisfying $|\alpha q_1 - p_1| > |\alpha q_2 - p_2| > |\alpha q_3 - p_3| > \cdots$.

6. These rational numbers thus offer a very good approximation to α relative to their denominators.

B. "World champion" approximations.

1. These observations lead to the notion of the "best rational approximations" to an irrational number α.

2. Given an irrational number α, we define the best rational approximations to α to be the complete list of rational numbers $p_1/q_1, p_2/q_2, p_3/q_3, \dots$, satisfying $|\alpha q_1 - p_1| > |\alpha q_2 - p_2| > |\alpha q_3 - p_3| > \cdots$.

3. In 1770 Joseph Lagrange proved that this list of best rational approximations is precisely the list of rational numbers found by truncating the continued fraction expansion for α.

4. Thus, the continued fraction expansion of a real number holds an incredibly important secret: its best rational approximations!

C. Truncating continued fractions.

1. If we wish to find the very best rational approximations of a real number α, we need only consider the fractions generated by truncating α's continued fraction expansion.

2. If we return to the golden ratio, $(1 + \sqrt{5})/2$, which has the endless continued fraction expansion [1, 1, 1, 1, 1, ...], then the best rational approximates to this special number are precisely those rationals having continued fractions [1, 1, 1, ... , 1].

3. We have already seen that these fractions are precisely the ratios of two consecutive Fibonacci numbers—the larger to the smaller.

II. Deriving a 12-note scale through number theory.

A. Ratios of pitches.

1. In Lecture Four, we described an octave as a musical interval between two pitches in which the two pitches have frequencies in a ratio of 2:1. An interval is a perfect fifth if the ratio of the frequencies of the two pitches is 3:2.
2. In Western music, the chromatic scale begins at one pitch—say, A—and progresses up in what are called half steps until it ends with the note that is one octave above the starting pitch. The pitches are derived from a geometric progression of perfect fifths starting with the first pitch and having a ratio $r = 3/2$.
3. For example, if we start at A (which is 440 Hz), we would produce: 440, $440 \times 3/2$, $440 \times (3/2)^2$, $440 \times (3/2)^3$, $440 \times (3/2)^4$, $440 \times (3/2)^5$, etc. We see the numbers 440, 660, 990, 1485, 2227.5, 3341.25, etc.
4. To keep the notes within the 440–880 Hz range, we divide the frequencies by 2 in order to lower the pitches so that they fall into the correct octave. This process requires us to modify our attractive geometric sequence.

B. So why do we end up with a 12-note chromatic scale?

1. Once we factor out the 440, the terms in our geometric progression have the form $1, 3/2, (3/2)^2, (3/2)^3, (3/2)^4, \ldots$. However, we also repeatedly divide by powers of 2. Our goal is to return to the same note, one octave higher. Thus we want to find a natural-number power q and a natural number p so that $(3/2)^q/2^p$ is ideally 1, or at least very, very close to 1. Notice that q represents the number of notes in our scale.
2. So, we wish to find natural numbers p and q so that $(3/2)^q$ is approximately equal to 2^p. In other words, $2^p \approx (3/2)^q$. If we translate this approximation into the equivalent statement involving a logarithm, then we would see $p \approx q\log_2(3/2)$.
3. Dividing by q, we see $p/q \approx \log_2(3/2)$; that is, we wish to find an excellent rational approximation p/q to the number $\log_2(3/2)$.
4. We first find the continued fraction expansion for $\log_2(3/2)$. Using the decimal expansion $\log_2(3/2) = 0.58496\ldots$, and a calculator, we can find that its continued fraction begins with $\log_2(3/2) = [0, 1, 1, 2, 2, 3, 1, 5, 2, 23, \ldots]$.

5. We can find the best rational approximations by truncating this expansion. First we would generate the rationals: 0/1, 1/1, 1/2, 3/5, 7/12, 24/41, ... The denominators are the q's and thus represent the number of notes in our chromatic scale. If we consider the approximation 7/12, then we can use a calculator to discover that $(3/2)^{12}/2^7 = 1.013\ldots$, which is very close to 1. So a 12-note chromatic scale would bring us nearly to our starting note, one octave higher.
6. Of course we could get even closer to 1 by using the approximation 24/41, but that would require a 41-note scale, which would not be practical. So the 12-note chromatic scale is the standard—and that 12, we now see, is a denominator of a best rational approximation! Music and number theory unite.
7. The fact that $(3/2)^{12}/2^7$ equals 1.013... and is not *exactly* equal to 1 is one reason why tuning musical instruments is so challenging.

III. The hidden patterns within quadratic numbers.

A. The quintessential quadratic numbers.

1. Quadratic irrational numbers are irrational numbers that are solutions to quadratic equations having integer coefficients—such as $4x^2 - 3x + 5 = 0$, or more generally, $ax^2 + bx + c = 0$, for integers a, b, and c.
2. As we have already seen, $\sqrt{2}$ is a quadratic irrational, and the golden ratio, $(1 + \sqrt{5})/2$, is a quadratic irrational.
3. We have also computed the continued fraction expansion for each of these quadratic irrational numbers. We found that $\sqrt{2} = [1, 2, 2, 2, \ldots]$ and $(1 + \sqrt{5})/2 = [1, 1, 1, 1, 1, \ldots]$. In each case we notice that the continued fractions are eventually periodic.

B. A search for structure.

1. Does this periodic pattern in the continued fraction hold for other quadratic irrational numbers? For insight, we consider the continued fraction expansions for other quadratic irrationals.
2. Using a calculator, we could confirm that: $\sqrt{3} = [1, 1, 2, 1, 2, 1, 2, \ldots]$; $\sqrt{5} = [2, 4, 4, 4, 4, \ldots]$; $\sqrt{6} = [2, 2, 4, 2, 4, 2, 4, \ldots]$; $\sqrt{7} = [2, 1, 1, 1, 4, 1, 1, 1, 4, \ldots]$; $\sqrt{23} = [4, 1, 3, 1, 8, 1, 3, 1, 8, \ldots]$.

3. In all these examples, the continued fraction expansion we find is periodic.

C. Lagrange's Theorem.

1. In fact, this observation holds in general for any real quadratic irrational and was first established by Joseph Lagrange in 1770. This result, known as *Lagrange's Theorem*, states that a real number has a periodic continued fraction expansion if and only if the real number is a real quadratic irrational.
2. If we consider the very complicated quadratic irrational $(4 - \sqrt{19})/3 = -0.119632\ldots$ and view its continued fraction expansion, we would see $[-1, 1, 7, 2, 1, 3, 1, 2, 8, 2, 1, 3, 1, 2, 8, \ldots]$ and notice that it too is periodic (with 2, 1, 3, 1, 2, 8 repeating forever).

D. Palindromes within periods.

1. Let us now return to the simple quadratic irrationals of the form $\sqrt{d}$, for some natural number d that is not a perfect square, and look a bit more closely at their continued fraction expansions.
2. Upon inspection we notice some amazing coincidences. First, the last number appearing in the repeated period is always equal to 2 times the first partial quotient.
3. Moreover, if we consider the period without that last term, we see that the list does not change if the period is read backward or forward; that is, the period without the last term is a numerical palindrome!
4. We see these assertions hold with the example $\sqrt{23} = [4, 1, 3, 1, 8, 1, 3, 1, 8, \ldots]$.
5. These amazing coincidences are, in fact, theorems. In particular, if d is a natural number that is not a perfect square, then the continued fraction for $\sqrt{d}$ will always become periodic after the very first partial quotient, the last number in the period will be twice the first partial quotient, and the period with the last number removed is always a palindrome.

IV. Returning to the Pell equation.

A. Searching for solutions to the Pell equation.

1. We now connect the amazing structure of the continued fraction of $\sqrt{d}$ with the Pell equation we studied in Lecture Thirteen.

2. The Pell equation has the generic form $x^2 - dy^2 = 1$, for which d is a given natural number that is not a perfect square. For example, $x^2 - 2y^2 = 1$. As with any Diophantine equation, we seek integer solutions, in this case, natural-number solutions.

B. A connection with quadratics.

1. Using $x^2 - 2y^2 = 1$ to illustrate the general theory, if we factor the left side, then our equation would become $(x - (\sqrt{2})y)(x + (\sqrt{2})y) = 1$. If we now divide by the second factor, we see $x - (\sqrt{2})y = 1/(x + (\sqrt{2})y)$; if we further assume that the size of x is approximately the size of y, then roughly speaking we can say $x - (\sqrt{2})y \approx 1/(y + (\sqrt{2})y)$—which if we divide both sides by y becomes $x/y - \sqrt{2} \approx 1/(1 + \sqrt{2})y^2$.
2. If we take the absolute value of both sides and introduce an inequality by discarding the number $(1 + \sqrt{2})$, then we would come upon the familiar-looking $|x/y - \sqrt{2}| < 1/y^2$, an inequality we saw earlier in Lecture Twenty-One that is satisfied by all the best rational approximations to $\sqrt{2}$.
3. Thus perhaps the solutions x and y that we seek for the Pell equation $x^2 - 2y^2 = 1$ come from the continued fraction expansion for $\sqrt{2}$.

C. Continued fractions and convergents.

1. We recall the continued fraction $\sqrt{2} = [1, 2, 2, 2, \ldots]$, and if we compute the best rational approximations by truncating this continued fraction, we see the list of rational approximants 1/1, 3/2, 7/5, 17/12, 41/29, 99/70, … .
2. If we consider these fractions as x/y and compute $x^2 - 2y^2$, then we see: $1^2 - (2 \times 1^2) = -1$; $3^2 - (2 \times 2^2) = 9 - 8 = 1$; $7^2 - (2 \times 5^2) = 49 - 50 = -1$; $17^2 - (2 \times 12^2) = 289 - 288 = 1$; $41^2 - (2 \times 29^2) = 1681 - 1682 = -1$; $99^2 - (2 \times 70^2) = 9801 - 9800 = 1$.
3. That is, every other best rational approximation gives rise to a solution to the Pell equation (and the other approximations give rise to solutions to the Pell equation $x^2 - 2y^2 = -1$).
4. In general, to find all solutions to $x^2 - dy^2 = 1$, we can first compute the continued fraction of $\sqrt{d}$ and then compute the rational numbers formed by truncating the continued fraction right at the end of the palindrome part (before the last term of the period, which equals twice the first partial quotient).

Those rational numbers x/y will form the *complete* list of all solutions x, y to the Pell equation $x^2 - dy^2 = 1$.

V. The many mysteries of continued fractions.

A. The continued fraction for π.

1. We have learned that the continued fraction expansions for quadratic irrational real numbers are eventually periodic. Now we wonder if there are other patterns in the continued fractions for other types of numbers.

2. We return to π and consider many, many partial quotients in its continued fraction expansion. Do you see a pattern?

3. $\pi = [3, 7, 15, 1, 292, \ldots, 436, \ldots, 20{,}776, \ldots]$.

4. There is no obvious pattern. If we just look at the largest partial quotient seen so far as we scan down the list of all those natural numbers, we see 3, 7, 15, 292, 436, and a little bit later, 20,776. Will these largest values get arbitrarily large, or is there a limit to their size? That is, are the partial quotients of π bounded or unbounded? The conjecture is that these numbers grow without bound.

B. The cube root of two.

1. Perhaps the chaotic-looking nature of the partial quotients of π arises from the fact that π is transcendental. To test this theory, we consider an algebraic number of degree 3; that is, a cubic irrational, $\sqrt[3]{2}$. Because this number is not a quadratic irrational (algebraic of degree 2), we know that its continued fraction expansion does not repeat. Perhaps there is a different type of easy pattern to uncover.

2. $\sqrt[3]{} = [1, 3, 1, 5, \ldots, 14, \ldots, 15, 3, 1, 4, 534, \ldots]$.

3. It appears just as chaotic looking as that of π. If we keep track of the largest partial quotients in this list, we see: 1, 3, 5, 14, 15, 534.

4. Is there a largest value in this list? That is, are the partial quotients for $\sqrt[3]{2}$ bounded or unbounded? The conjecture is that these numbers grow without any bound, but no one can prove or disprove this claim.

5. Let us notice that in both the continued fraction expansions for π and $\sqrt[3]{2}$ we see that 1 appears more often than any other number. This observation turns out to be reasonable in light of a very deep result about continued fractions. We will describe this result in our final lecture.

Questions to Consider:

1. Recall that $\sqrt{5}$ has the continued fraction expansion $[2, 4, 4, 4, 4, \ldots]$, so the first best rational approximant is $2/1 = 2$. Find the next three best rational approximants.

2. Use your answers to Question 1 above to find a few solutions to the Pell equation $x^2 - 5y^2 = 1$.

Lecture Twenty-Four
A Journey's End and the Journey Ahead

Scope: In this final lecture we take a step back to view the entire panorama of number theory, seeing it as the art of not only looking up at the entire sky of numbers but also looking down to earth, at the detail within the numerical terrain at our feet. We will open with the continued fraction expansions for almost all numbers. We will then consider the growth of partial quotients within the context of quadratic irrational numbers and Liouville-type numbers. We will also highlight an attractive result of Erdös's and its recent generalizations as we take a final look at the entire mosaic of number theory that we have created. We will highlight some of the synergistic moments in which seemingly unrelated ideas came together to tell a unified story of number. Finally, we will look beyond the number theory and mathematics and celebrate the underlying theme of creativity and originality that made our entire journey possible. Here we will explore this mind-set and how it has a transformative effect, not just within the narrow, endless confines of number, but within the boundless possibilities of our lives and imagination.

Outline

I. The continued fraction expansion for almost all numbers.
  A. Continued fractions as the digital DNA of real numbers.
    1. We have seen in the past few lectures that to truly understand the number theoretic structure of real numbers, we should consider the continued fraction representation.
    2. In some sense, the numbers that make up the continued fraction expansion for α—the so-called *partial quotients*—hold α's digital DNA.
    3. For example, truncating the continued fraction expansion produces the complete list of best rational approximations to that real number.
  B. Structure and chaos within continued fractions.
    1. The partial quotients can reveal features of the number α itself.

    2. For example, the partial quotients of α form an endless list if and only if α is an irrational number.
    3. The partial quotients of α eventually become periodic and repeat if and only if α is a real quadratic irrational number.
    4. The partial quotients for Euler's e have a very easy-to-identify pattern: $e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, \ldots]$.
    5. The partial quotients for π, however, exhibit no obvious pattern and appear to be chaotic in nature.
  C. The continued fraction expansions for random real numbers.
    1. Suppose we were to pick a real number at random, let us call it α. We noted in Lecture Twenty that a real number selected at random will be a transcendental number with probability 100%, so we are confident that the continued fraction expansion for the random α will *not* be periodic (because periodic implies quadratic, which in turn implies algebraic).
    2. What values for the partial quotients might we expect to see? Recall that the partial quotients are defined to be the integer part of the reciprocal of a previous fractional part.
    3. Since a fractional part of any number is between 0 and 1, let us imagine selecting a random number between 0 and 1. If we consider its reciprocal and then the integer part of that reciprocal, what would we find?
    4. If our fractional part falls within the subinterval between 1/2 and 1, then the integer part of the reciprocal will be 1. For example, consider the fractional part 0.6. Its reciprocal is 10/6, which equals 5/3, which equals 1.6666... . The integer part is 1!
    5. We would guess that if these fractional parts were being selected at random from the interval between 0 and 1, about half of them would have reciprocals that have integer parts equal to 1.
    6. If our fractional part falls within the subinterval between 1/3 and 1/2, then the integer part of the reciprocal will equal 2. For example, consider the number 0.35. Its reciprocal is 100/35, which equals 2.857... . Notice the integer part is indeed 2.
    7. Thus we would guess that about 1/6 (which is 1/2 − 1/3) of the partial quotients should equal 2.

8. This pattern continues: With smaller and smaller likelihoods, we would expect to see larger and larger integer parts (that is, larger and larger partial quotients).
9. These informal observations can be made precise and are quantified in a result known as the *Gauss-Kuz'min distribution*: If we select a random real number and consider its continued fraction expansion, then within the partial quotients we would expect to see every natural number appearing infinitely often, with the most popular number being 1, then 2, then 3, and so on.
10. More precisely, the probability of seeing the partial quotient 1 is roughly 42%, the probability of seeing the partial quotient 2 is about 16.9%, the probability of seeing 3 is about 9%, etc.

II. Sizing up the partial quotients.

A. Badly approximable numbers.

1. Given our previous observations and the Gauss-Kuz'min distribution, we would expect to see a great many 1s appearing in the continued fraction expansion for a random real number.
2. Notice that we see many 1s appearing in the first few terms of the continued fraction expansion for π.
3. However, for a random real number we now see that the partial quotients grow without bound, while we do not know if the partial quotients for π are bounded or unbounded.
4. Very large partial quotients give rise to surprisingly close rational approximations.
5. If the partial quotients of a real number α are bounded—that is, they are all less than or equal to a fixed value—then α is called a *badly approximable number*.
6. This name follows since small partial quotients prevent the best rational approximations from getting *too* close to α *too* fast.
7. Real quadratic irrational numbers are badly approximable, and the most badly approximable number of all is the golden ratio.

B. Liouville numbers.

1. Liouville numbers are real numbers that have incredibly close rational approximations with relatively modest denominators, a property that led to Liouville's proof that these numbers are transcendental (Lecture Twenty).
2. The fact that Liouville numbers have such excellent rational approximations implies that Liouville numbers have partial quotients that grow dramatically and without any bound. In some sense, they are the opposite of badly approximable numbers.
3. It turns out that Liouville numbers have *such* amazing rational approximations that they are extremely rare. If we pick a number at random, it is with probability 0% that we accidentally select a Liouville number.

C. A theorem of Erdös's and recent results.

1. In 1962, Erdös gave a very clever argument showing that even though the Liouville numbers are extremely rare, every real number can be written as the sum of two Liouville numbers.
2. About 35 years later, in 1996, I was able to generalize Erdös's result and show that given any nontrivial function of two variables, call it $f(x,y)$ and any real number α, we can find two Liouville numbers x and y such that $f(x,y) = \alpha$.
3. If $f(x,y) = x + y$, then we have Erdös's original result as this very special case.

III. A look back at the number mosaic.

A. Thales of Miletus.

1. Thales was a pre-Socratic philosopher and scholar from around 600 B.C.E. who was one of Pythagoras's teachers.
2. Toward the end of his life, Thales dedicated himself to the study of astronomy. As the tale goes, one evening Thales was staring up at the stars as he took a stroll, and he fell into a ditch.
3. His woman attendant looked at this great scholar who had just fallen down and asked, How can you know what is happening in the heavens when you do not see what is at your feet?
4. Here we highlight some great moments from our journey together—both the amazing results now at our feet, as well as the heavenly panoramic that allows us to appreciate all the surprising interconnections that make these results a reality.

B. Personalizing powers of 2.
   1. At the opening of the course, we wondered if there existed a power of 2 whose first few digits when read left to right would coincide with our own social security numbers.
   2. More generally, we wondered if given any natural number A, there existed a natural number B such that the left-most digits of 2^B agreed with the digits of A.
   3. Upon first inspection, this question appeared out of reach, however once we extended our reach into the world of irrational numbers, we discovered Kronecker's Theorem.
   4. Kronecker's Theorem told us that the fractional parts of multiples of irrational numbers are dense within the interval between 0 and 1. This fact, together with our proof that log 2 is irrational, is enough to prove that powers of 2 can begin with any prefix we desire.
   5. To prove a theorem about natural numbers, we had to venture into the mysterious and strange world of irrationality.

C. The 12-note chromatic scale.
   1. We first encountered the issues involving the chromatic scale in our discussion of geometric progressions—progressions of numbers whose ratios of consecutive terms are constant.
   2. In order to understand why the chromatic scale contains 12 notes, we required best rational approximations to an irrational number $\log_2(3/2)$.
   3. Thus, to derive the length of 12 notes, we required the continued fraction expansion of this auxiliary irrational number.
   4. So we answered a musical question involving geometric progressions and ratios using the theory of irrational numbers, continued fractions, and best rational approximants.

D. Algebraic number theory was born from a mistake.
   1. Fermat's Last Theorem was the inspiration for Lamé's clever but incorrect proof.
   2. Lamé assumed that certain algebraic integers behaved like the ordinary integers—in particular, that they possessed the unique factorization property that Euclid had established centuries earlier.
   3. Unfortunately, Lamé's algebraic integers do not exhibit the unique factorization property.

   4. Kummer was then inspired to discover ideals—packets of algebraic integers—that do exhibit unique factorization into prime packets.
   5. This beautiful insight gave birth to algebraic number theory.

E. Primes, imaginary numbers, rational solutions, and geometry.
   1. Prime number theory focuses on the structure of the fundamental multiplicative building blocks of the natural numbers: 2, 3, 5, 7, 11, … .
   2. However, to understand their nuanced properties, as in the prime number theorem or in the Riemann Hypothesis, we are required to journey into the complex world of imaginary numbers.
   3. To find integer or rational solutions to certain Diophantine equations, we discovered that a rich structure is revealed through the study of curves and their intersections with lines.
   4. Thus we see the powerful marriage between geometry and arithmetic, which gave birth to algebraic geometry.

IV. Number theory as a metaphor for discovery and creativity.

A. The world of diverse ideas is a connected whole.
   1. One theme we have seen again and again is that notions that first appear to be disconnected and unrelated are in fact inextricably intertwined.
   2. As our understanding of nature and number deepens, objects that first appeared different become interconnected.
   3. It is these deep interconnections that allow us to move the frontiers of discovery forward.

B. How do we move the boundaries of our creativity and understanding forward?
   1. Mathematics in general, and number theory in particular, requires us to create.
   2. Mathematicians are at once artists creating imaginative ideas and also explorers trying to understand truth within our universe—both the concrete and abstract world around us.

C. Life lessons that transcend the numbers.
   1. The mind-set that allows us to advance the frontiers of number theory also empowers us to expand our own boundaries.

2. We can be more creative and imaginative by deliberate intent through certain habits of thinking that we employed in our journey through number theory.
3. I close this course with my "top 10" list of life lessons that are constants within our creative journey through mathematics and can be constants through our entire lives.
   - **a.** Just do it.
   - **b.** Make mistakes and fail, but never give up.
   - **c.** Keep an open mind.
   - **d.** Explore the consequences of new ideas.
   - **e.** Seek the essential.
   - **f.** Understand the issue.
   - **g.** Understand simple things deeply.
   - **h.** Break difficult problems into easier ones.
   - **i.** Examine issues from different points of view.
   - **j.** Look for patterns and similarities.

D. The limitless nature of numbers and our imaginations.
1. Using our imagination and creativity, we can conquer any challenge we elect to face.
2. Looking at our world through the lens of number theory, we see everything with greater clarity and in vibrant color.

Questions to Consider:

1. How would you describe the mathematical discipline known as number theory?
2. What was your favorite number theory result or fact that you learned in this course? What was the most perplexing?

Timeline

B.C.E.

c. 2000–1650 ..... Babylonians apply the Pythagorean Theorem to approximate the square root of 2.

c. 540 ..... Pythagoras founds his school and proves the Pythagorean Theorem.

c. 540–500 ..... Pythagoreans confounded by their proof that irrational numbers exist.

c. 300 ..... Euclid presents his axiomatic method for geometry in *Elements*, in which he proves the infinitude of primes, the irrationality of the square root of 2, and the fundamental theorem of arithmetic. He also presents the Euclidean algorithm for finding the greatest common factor of two natural numbers, perhaps the first algorithm ever created.

c. 200 ..... Eratosthenes develops his "sieve" for finding prime numbers up to a given value.

C.E.

c. 200–300 ..... Early study of cycles of remainders by Chinese mathematicians that foreshadowed the notion of modular arithmetic.

c. 210–290 ..... Diophantus writes the first books on algebra in his 13-volume work *Arithmetica*.

1202 ..... Fibonacci explicitly describes the Fibonacci sequence.

1570 ..... Bombelli translates Diophantus's *Arithmetica* into Latin, the first step

toward making his fundamental work on equations accessible to European scholars.

1575 ..... Xylander's Latin translation of *Arithmetica* is the first to be published.

1637 ..... Fermat asserts what became known as his "Last Theorem" in the margin of his copy of *Arithmetica*.

1640 ..... Fermat asserts his Little Theorem in a letter.

1736 ..... Euler gives the first complete published proof of Fermat's Little Theorem.

1737 ..... Euler establishes his product formula, marking the beginning of modern analytic number theory.

1742 ..... Goldbach conjectures that every natural number greater than 4 can be written as the sum of two primes.

c. 1750 ..... Euler uses Fermat's method of descent to show that Fermat's Last Theorem is true for $n = 3$.

1770 ..... Lagrange proves that the best rational approximations to an irrational number can be obtained from its continued fraction expansion. He also shows that a real number has a periodic continued fraction expansion if and only if the real number is a real quadratic irrational.

c. 1785 ..... Eight-year-old Gauss is said to derive a formula for the sum of the first n natural numbers.

c. 1792 ..... Legendre and Gauss conjecture the statement that later became known as the *prime number theorem*.

1801 ..... Gauss introduces modular arithmetic.

c. 1820 ..... Germain makes important progress on Fermat's Last Theorem.

1825 ..... Dirichlet and Legendre use ideas of Germain to prove Fermat's Last Theorem holds for $n = 5$.

1837 ..... Dirichlet proves result on prime numbers appearing in arithmetic progressions.

1839 ..... Lamé claims to have a proof of Fermat's Last Theorem, but it is flawed.

1842 ..... Dirichlet proves his theorem about rational approximations to real numbers. This work and Liouville's work of 1844 mark the dawn of the area of number theory called *Diophantine approximation*.

1843 ..... Binet derives a formula for the n^{th} Fibonacci number. Kummer uses ideas in Lamé's attempt to prove Fermat's Last Theorem to develop groundbreaking work that marks the birth of algebraic number theory.

1844 ..... Liouville constructs the first examples of transcendental numbers. He also proves his theorem about the size of denominators of rational numbers that closely approximate algebraic numbers.

1847 ..... Kummer extends the ideas of Euler, Germain, Dirichlet, Legendre, and others to prove that Fermat's Last Theorem is true for all "regular prime" exponents.

1850 ..... Chebyshev makes progress on a proof of the prime number theorem.

1859 ..... Riemann publishes his seminal paper relating the as-yet-unproven prime number theorem to complex numbers and Euler's product formula. He proposes what became known as the now-famous Riemann Hypothesis.

1873 ..... Hermite proves that e is transcendental.

1882 ..... Lindemann proves that π is transcendental.

1883 ..... Lucas invents the popular Tower of Hanoi puzzle, whose solution involves a recurrence sequence.

1884 ..... Kronecker proves that the fractional parts of integer multiples of any irrational number are dense in the interval from 0 to 1.

1896 ..... Hadamard and Poussin independently prove the prime number theorem.

1900 ..... Hilbert poses 23 questions at the Second International Congress of Mathematics in Paris as a challenge for the 20th century. Many have been solved to date; they are considered milestones.

1921 ..... Mordell makes several seminal discoveries on the algebraic structure of rational points on elliptic curves.

1933 ..... Skewes number is the largest ever used in a proof (at that time).

c. 1934 ..... Gelfond-Schneider Theorem asserting the transcendence of certain numbers is proved.

1937 ..... Collatz poses his conjecture on the behavior of a particular sequence of numbers.

1949 ..... Erdös and Selberg each publish proofs of the prime number theorem that use only elementary techniques.

1962 ..... Erdös proves that every real number can be written as the sum of two Liouville numbers.

1970 ..... Matiyasevich proves there cannot exist a general algorithm that will determine in a finite number of steps if an arbitrary Diophantine equation has an integer solution, answering one of Hilbert's 23 questions.

1977 ..... Rivest, Shamir, and Adleman create a public key cryptography system known as RSA encryption. Mazur produces several seminal results involving the algebraic structure of rational points on elliptic curves.

1983 ..... Faltings proves the Mordell conjecture and later wins a Fields Medal.

1993 ..... Wiles proves Fermat's Last Theorem, but an error is uncovered.

1994 ..... Wiles completes a correct proof of Fermat's Last Theorem.

Glossary

absolute value: The distance of a real number from zero on the number line.

additive identity: Zero is the additive identity because $a + 0 = a$ for any number a.

additive inverse: The additive inverse of a number a is $-a$, because $a + -a = 0$, the additive identity. For example, the additive inverse of 5 is -5, and the additive inverse of -17 is $-(-17) = 17$.

algebra: The branch of mathematics that studies equations, their solutions, and their underlying structures.

algebraic geometry: The branch of mathematics that combines ideas from algebra and geometry, with many questions motivated by the need to understand integer solutions to equations.

algebraic integers: A generalization of integers involving algebraic numbers such as $4 + 3i$ or $2 + 6\sqrt{5}$.

algebraic number theory: The branch of number theory that studies numbers that are solutions to certain polynomial equations.

algebraic numbers: The collection of all numbers that are solutions to nontrivial polynomials with integer coefficients.

almost all: A portion of a collection is said to be "almost all" of that collection if when an item is selected at random from the entire collection the chance of choosing something inside that portion is mathematically 100%.

analysis: The branch of mathematics that generalizes the ideas from calculus, especially notions of distance and continuous change.

analytic number theory: The branch of number theory that studies the integers (especially primes) using ideas from calculus and analysis.

arithmetic progression: A list of numbers in which the difference between any number and its successor is always the same value.

ascent, Fermat's method of: A method by which one integer solution to a Diophantine equation gives rise to infinitely many integer solutions.

axiom: A fundamental mathematical statement that is accepted as true without rigorous proof.

best rational approximants: The sequence of rational numbers that approximate a given real number as closely as possible in terms of the size of the denominators.

Binet formula: A formula for the n^{th} Fibonacci number:

$$F_n = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{\sqrt{5}}.$$

calculus: The branch of mathematics that studies continuous processes and instantaneous rates of change based on precise measures of distance.

chromatic scale: A sequence of 12 pitches in Western music that starts at one pitch and increases frequency of each pitch at regular intervals until reaching the pitch an octave higher.

coefficient: In a polynomial, a coefficient is the number multiplied by a power of the unknown. For example, in the polynomial $27x^8 + 7x^3 - 8x$, 27 is the coefficient of x^8.

Collatz conjecture: A conjecture made in 1937 by Lothar Collatz that a particular algebraic process always terminates at the value 1, regardless of the starting value.

complex numbers: The collection of all numbers of the form $x + yi$, where x and y can equal any real number and i is the square root of -1.

complex plane: A representation of the complex numbers, consisting of a plane with horizontal (real) and vertical (imaginary) axes meeting at a right angle at a point called the "origin."

composite number: A natural number greater than 1 that can be written as the product of two smaller natural numbers.

conjecture: A mathematical statement thought to be true but for which a rigorous proof has not yet been found.

continued fraction: A method of writing real numbers as nested fractions within fractions where all the numerators equal 1.

converge: An infinite series is said to converge if the endless sum has a numerical value. A geometric series converges if the ratio of each term to its successor is less than 1 in absolute value.

counting numbers: The collection of numbers 1, 2, 3, 4, 5, and so on. Also called the "natural numbers."

decimal expansion: The representation of a number in base 10. A decimal point separates the places representing 1s, 10s, 100s, and so on, to the left, and the $1/10^{\text{th}}$s, $1/100^{\text{th}}$s, and so on, to the right.

degree of an algebraic number: The smallest degree possible of a polynomial in an equation for which the algebraic number is a solution.

degree of polynomial: The largest exponent that appears in the polynomial. For example, the polynomial $7x^3 - 5x + 2$ has degree 3.

dense: The rational numbers are dense within the real numbers because between any two distinct real numbers, there is at least one rational number.

descent, Fermat's method of: A method used to show certain Diophantine equations have no integer solutions.

Diophantine approximation: An area of number theory in which one studies how well irrational numbers can be approximated by rational numbers.

Diophantine equation: An equation that involves only addition, subtraction, and multiplication of natural numbers and unknowns, for which integer solutions are sought.

disjoint: Having no elements in common.

distributive law: The arithmetic law that states that $a \times (b + c) = (a \times b) + (a \times c)$, for numbers a, b, and c.

diverge: An infinite series is said to diverge if the endless sum has no meaningful numerical value. The harmonic series $1 + 1/2 + 1/3 + 1/4 + \cdots$ diverges.

division algorithm: A systematized version of "long division" used to find the quotient and remainder when one integer is divided into another.

e: The fundamental parameter in the measure of growth. The value of e is 2.71828... and is equal to the limiting value of the expression $(1 + 1/n)^n$ as n grows without bound.

elementary number theory: The area of number theory that focuses on fundamental questions about numbers and whose often subtle answers do not involve advanced mathematics.

elliptic curve: A graph of the cubic equation given by $y^2 = x^3 + ax + b$, where a and b are given integers.

equation: An expression that sets two quantities equal. For example, $2 + 2 = 4$ and $x^2 - 2 = 0$ are equations.

Euclidean algorithm: An algorithm that produces the greatest common factor of two natural numbers. The method involves repeated applications of the division algorithm.

Euler's product formula:

$$\left(\frac{1}{1-1/2}\right)\times\left(\frac{1}{1-1/3}\right)\times\left(\frac{1}{1-1/5}\right)\times\left(\frac{1}{1-1/7}\right)\times\left(\frac{1}{1-1/11}\right)\times\cdots$$
$$= 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \cdots$$

exponent: A superscript following a number or variable. For example: $2^3 = 2 \times 2 \times 2$. Also called a "power."

factor: A natural number m is a factor of an integer n if m divides evenly into n.

Fermat's Last Theorem: Given any fixed natural number exponent n greater than 2, there are no natural-number solutions for x, y, z to the equation $x^n + y^n = z^n$.

Fermat's Little Theorem: Given a prime number p and any natural number a that is relatively prime to p, when we divide $a^{(p-1)}$ by p, the remainder equals 1.

Fibonacci numbers: The sequence of numbers 1, 1, 2, 3, 5, 8, and so on, in which each number after the first two is equal to the sum of its two predecessors.

Fields Medal: An award given every four years to two to four mathematicians under the age of 40 by the International Mathematics Union. Considered by many to be the equivalent of a Nobel Prize, which does not exist for math.

fractional part: The decimal part of a real number. For example, the fractional part of 3.14159 is 0.14159.

fundamental theorem of arithmetic: Every natural number greater than 1 can be written uniquely—up to reordering of the factors—as a product of prime numbers.

Gelfond-Schneider Theorem: If an algebraic number not equal to 0 or 1 is raised to an algebraic irrational power, then the result is a transcendental number.

geometric progression: A list of numbers in which any number divided by its successor always gives the same value.

geometric series: The endless sum of all the numbers in a geometric progression.

Germain prime: A prime number p for which the number $2p + 1$ is also prime.

Goldbach conjecture: Goldbach's conjecture states that every even number greater than 4 equals the sum of two primes.

golden ratio: The number $(1+\sqrt{5})/2$.

greatest common factor: The greatest common factor of two natural numbers is the largest natural number that divides evenly into each of them.

group: A collection of elements and an operation for combining them that satisfies certain special algebraic properties.

harmonic series: The infinite series $1 + 1/2 + 1/3 + 1/4 + 1/5 + \cdots$.

Hilbert's problems: The list of open questions David Hilbert posed at the Congress of Mathematics in 1900. He considered them to be the most important open questions in mathematics for the 20th century.

i: The square root of -1.

ideal: A packet of algebraic integers that exhibits unique factorization into prime ideals.

imaginary numbers: The collection of numbers that are multiples of i.

infinite series: An unending sum of quantities such as $1 + 1/2 + 1/4 + 1/8 + 1/16 + \cdots$. Such a sum may or may not have a numerical value.

integers: The collection of numbers consisting of the natural numbers 1, 2, 3, ... , together with all their negatives and zero.

irrational numbers: The collection of all numbers that are not rational.

Lagrange's Theorem: A real number has a periodic continued fraction expansion if and only if the real number is a real quadratic irrational.

logarithm: The exponent to which a base must be raised to produce a given number. For example, the base-10 logarithm of 1000 is 3, because $10^3 = 1000$.

Lucas sequence: The sequence of numbers 2, 1, 3, 4, 7, 11, and so on, in which each number is the sum of its two predecessors.

multiplicative identity: The number 1 is the multiplicative identity because $1 \times a = a$ for any number a.

multiplicative inverse: The multiplicative inverse of a nonzero number a is its reciprocal, $1/a$, because $a \times 1/a = 1$, the multiplicative identity. For example, the multiplicative inverse of 5 is 1/5, and the multiplicative inverse of 1/2 is 2.

natural numbers: The collection of numbers 1, 2, 3, 4, 5 ...; also called the "counting numbers."

nonrepeating expansion: A number expansion in any base is nonrepeating if it is not periodic.

number line: A representation of the real numbers; a line extending endlessly in both directions, with a point marked as 0 and at least one more point, usually 1, marking the unit of length. Each point on the line corresponds to a real number according to its distance from 0, with points to the right of zero denoting positive numbers and points to the left of zero denoting negative numbers.

number theory: The area of mathematics that focuses on the properties and structure of numbers.

octave: An interval in music where the two pitches have a frequency ratio of 2 to 1.

partial quotients: The natural numbers appearing in a continued fraction expansion.

Pell equation: A Diophantine equation of the form $x^2 - dy^2 = 1$, where d is a given square-free natural number.

perfect fifth: An interval in music in which the two pitches have a frequency ratio of 3 to 2.

periodic expansion: A number expansion in any base is periodic if, eventually, the digits to the right of the decimal point fall into a pattern that repeats forever. Also known as "repeating expansion."

pi: The ratio of the circumference of a circle to its diameter. Pi is denoted by the Greek letter π and equals 3.14159... .

$\pi(n)$: The number of primes less than or equal to the natural number n.

Pigeonhole Principle: The basic but extremely important observation that placing $n + 1$ objects into n pigeonholes results in at least one pigeonhole having two or more objects.

polynomial: An expression involving a single unknown (usually denoted by x), in which various powers of the unknown are multiplied by numbers and then added. For example, $3x^2 - 17x + 5$ and $27x^8 + 7x^3 - 8x$ are polynomials.

prime factorization: Calculation of all the prime factors in a number.

prime number: A natural number greater than 1 that cannot be written as the product of two smaller natural numbers.

prime number theorem: The number of primes less than or equal to a particular natural number n is approximately $ln(n)/n$, where $ln(n)$ denotes the natural logarithm of n. That is, as n increases without bound, the number of primes less than n gets arbitrarily close to $ln(n)/n$.

proof: A sequence of logical assertions, each following from the previous ones, that establishes the truth of a mathematical statement.

public key cryptography: A method of encoding and decoding messages in which the encoding process can be announced publicly.

Pythagorean Theorem: $a^2 + b^2 = c^2$, given a right triangle with side lengths a, b, and c (with c the longest length—the hypotenuse).

Pythagorean triple: A trio of numbers x, y, and z that satisfies the Pythagorean Theorem. The trio 3, 4, 5 is a Pythagorean triple.

ratio: A quantity that compares two measurements by dividing one into the other.

rational numbers: The collection of numbers consisting of all fractions (ratios) of integers with nonzero denominators.

rational point: A point (X, Y) in the coordinate plane for which the X and Y values are both rational numbers.

real numbers: The collection of all decimal numbers, which together make up the real number line.

recurrence sequence: A list of numbers in which, given one or more starting values, subsequent values are produced from preceding values using a given rule.

relatively prime: Two natural numbers are relatively prime if 1 is the largest natural number that divides evenly into both of them; that is, their greatest common factor is 1.

repeating expansion: See "periodic expansion."

Riemann Hypothesis: A conjecture involving the complex number solutions to a particular equation. If true, the Riemann Hypothesis has important implications about the distribution of prime numbers. A prize of $1 million has been offered for a complete proof.

RSA encryption: A popular method of public key cryptography developed by Rivest, Shamir, and Adleman that uses Fermat's Little Theorem.

scytale: A tool used by ancient Greeks to encrypt and decrypt messages.

Sieve of Eratosthenes: A process by which the prime numbers up to a given value can be found.

Skewes number: A number approximately equal to $10^{10^{10^{34}}}$.

slope: The pitch of a line, defined precisely as the ratio of the change in the vertical direction of the line to the change in the horizontal direction.

solution: Given an equation involving an unknown, a number is a solution to the equation if substituting that value for the unknown yields a valid equation.

square root: The square root of a number is a number that when multiplied by itself yields the first number.

square root of 2: $\sqrt{2}$, which equals 1.414... .

square-free number: A natural number whose prime factorization does not contain any particular prime more than once.

theorem: A mathematical statement that has been proven true using rigorous logical reasoning.

Towers of Hanoi: A puzzle consisting of three pegs and a stack of disks of graduated sizes on one peg which are to be transferred to another peg following certain rules.

transcendental numbers: The collection of all numbers that are not algebraic.

triangular numbers: The series of numbers formed by successive sums of the terms of an arithmetic progression, with the first term being 1 and the common difference being 1. The sum $1 + 2 + 3 + \cdots + n$ is the n^{th} triangular number. The first few triangular numbers are 1, 3, 6, 10, 15, and 21.

twin prime conjecture: There are infinitely many twin primes. Two prime numbers are twin primes if their difference is 2.

unique factorization: Every natural number greater than 1 can be written as a product of prime numbers in only one way, up to a reordering of the factors. This product of primes is the unique factorization of the number.

unit circle: The circle of radius 1 centered at the origin; algebraically, it is the collection of all points (X, Y) satisfying the equation $X^2 + Y^2 = 1$.

Biographical Notes

Adleman, Leonard (1945–). This theoretical computer scientist from the University of Southern California studies cryptography and molecular biology. Together with Ronald Rivest and Adi Shamir in 1977, he created a method of public key encryption known as the RSA algorithm.

Bertrand, Joseph (1822–1900). A French mathematician at the École Polytechnique and other schools, Bertrand made contributions in probability and mechanics, as well as his famous conjecture made in 1845 that there is always a prime between n and $2n$.

Binet, Jacques (1786–1856). This French mathematician worked in number theory and matrix theory. The closed form expression for the Fibonacci numbers is named after him.

Cantor, Georg (1845–1918). A German mathematician of Russian heritage and a student of Karl Weierstrass, Cantor established many of the early fundamentals of set theory. Between 1874 and 1884, he created precise ways to compare infinite sets, establishing the existence of infinitely many sizes of infinity, as well as infinitely many irrational and transcendental numbers. The controversy stirred by his work, along with bouts of depression and mental illness, caused him great difficulties later in his life, and he died in a sanatorium.

Chebyshev, Pafnuty (1821–1894). This Russian mathematician proved Bertrand's conjecture that there is always a prime between n and $2n$. His work also contributed to later proofs of the prime number theorem.

Collatz, Lothar (1910–1990). A German mathematician at the University of Hamburg, Collatz may be best known for the Collatz conjecture, which he posed in 1937 and which remains unsolved. He died while attending a math conference.

Diophantus (c. 210–290 C.E.). This Greek mathematician lived in Alexandria, Egypt, where he wrote one of the earliest treatises on solving equations, *Arithmetica*. Although he considered negative numbers to be absurd and did not have a notation for zero, he was one of the first to consider fractions as numbers. In modern number theory, Diophantine analysis is the study of equations with integer coefficients for which integer solutions are sought.

Dirichlet, Johann (1805–1859). A German mathematician at the University of Berlin, Dirichlet made many contributions to number theory, including important work on the distribution of primes and rational approximations. His wife was a sister of composer Felix Mendelssohn.

Eratosthenes (c. 276–194 B.C.E.). A Greek scholar who lived in Egypt, Eratosthenes was a mathematician, geographer, astronomer, and poet. The "sieve" that bears his name is a method for extracting primes from a list of consecutive numbers.

Erdös, Paul (1913–1996). An immensely prolific Hungarian mathematician, Erdös authored or coauthored approximately 1500 papers. Choosing to have no formal professional position, he traveled from institution to institution to work with colleagues in number theory, probability, set theory, combinatorics, and graph theory. He discovered remarkably "elementary" proofs of the Bertrand conjecture and, using a result of Atle Selberg, the prime number theorem.

Euclid (c. 325–265 B.C.E.). The mathematician Euclid lived in Alexandria, Egypt, and his major achievement was *Elements*, a set of 13 books on basic geometry and number theory. His work and style is still fundamental today, and his proofs of the infinitude of primes and the irrationality of $\sqrt{2}$ are considered two of the most elegant arguments in all of mathematics.

Euler, Leonhard (1707–1783). A Swiss mathematician and scientist, Euler was one of the most prolific mathematicians of all time. He introduced standardized notation and contributed unique ideas to all areas of analysis, especially infinite sum formulas for sine, cosine, and e^x. The equation known as Euler's formula, $e^{\pi i} + 1 = 0$, is considered by many to be the most beautiful in all mathematics.

Fermat, Pierre de (1601–1665). This French lawyer was one of the best mathematicians of his time. Sometimes called the creator of modern number theory, Fermat's contributions are numerous, including his so-called "Little Theorem," famous "Last Theorem," and his methods of ascent and descent for analyzing Diophantine equations.

Fibonacci, Leonardo de Pisa (c. 1175–1250). An Italian mathematician, Fibonacci traveled extensively as a merchant in his early life. Perhaps the best mathematician of the 13th century, he introduced the Hindu-Arabic numeral system to Europe and discovered the special sequence of numbers that bears his name.

Gauss, Carl Friedrich (1777–1855). A German mathematician commonly considered the world's best mathematician, Gauss is known as the "Prince of Mathematics." He established mathematical rigor as the standard of proof and provided the first complete proof that complex numbers are algebraically closed, meaning that every polynomial equation with complex coefficients has its solutions among complex numbers.

Germain, Sophie (1776–1831). This French mathematician battled social pressure and discrimination to become one of the most highly regarded women mathematicians of her day. She often wrote using a male pseudonym, but she was admired and mentored by Lagrange and Gauss even more after they discovered she was a woman. She made significant progress on Fermat's Last Theorem and the study of primes, including a particular variety that now bears her name.

Goldbach, Christian (1690–1764). This Prussian-born mathematician is perhaps best known for a conjecture he made in a letter to Euler. The Goldbach conjecture, which claims that every even number greater than 2 can be written as the sum of two primes, is one of the oldest unsolved problems in number theory.

Hadamard, Jacques-Salomon (1865–1963). This French mathematician independently produced a proof of the prime number theorem in 1896, the same year that Charles de la Vallée-Poussin also produced a proof.

Hilbert, David (1862–1943). Born in Prussia, this German mathematician was one of the most broadly accomplished and widely influential in the late 19th century and 20th century. He spent most of his professional life at the University of Göttingen, a top center for mathematical research. His presentation in 1900 of unsolved problems to the International Congress of Mathematics is considered to be one of the most important speeches ever given in mathematics. He was a vocal supporter of Georg Cantor's work and presented the Continuum Hypothesis as the first problem on his list in 1900.

Hopper, Grace Murray (1906–1992). An American mathematician, Hopper was a pioneer in the early days of computer science, writing the first compiler for a computer programming language. She spent most of her career in the Navy and retired at the rank of rear admiral.

Kronecker, Leopold (1823–1891). This German mathematician made contributions in number theory, algebra, and analytic ideas of continuity.

As an analyst and logician, he believed that all arithmetic and analysis should be based on the integers and, thus, did not believe in the irrational numbers. This put him at odds with a number of colleagues and, especially, the new ideas of Cantor in the 1870s.

Kummer, Ernst (1810–1893). This German mathematician developed the notion of ideal numbers by exploring the property of unique factorization mistakenly assumed in Lamé's flawed proof of Fermat's Last Theorem.

Lagrange, Joseph-Louis (1736–1813). This French-Italian mathematician was a student of Euler and was considered one of the best mathematicians of his day. He made numerous contributions to number theory, including the theory of continued fractions.

Lamé, Gabriel (1795–1870). This French mathematician made important contributions in number theory. He proved Fermat's Last Theorem for $n = 7$. His clever but flawed attempt at a general proof led to important developments in number theory.

Legendre, Adrien-Marie (1752–1833). This French mathematician made important contributions in number theory, statistics, algebra, and analysis. He proved Fermat's Last Theorem for $n = 5$ independently of and shortly after Dirichlet, and he conjectured the prime number theorem in 1796.

Liouville, Joseph (1809–1882). This French mathematician worked in many fields but is perhaps best known for his proof, given in 1844, of the existence of transcendental numbers. He constructed actual examples and described a special class of transcendental numbers that are now called *Liouville numbers*.

Littlewood, John (1885–1977). This British mathematician made contributions in number theory related to the prime number theorem and the Riemann Hypothesis.

Lucas, Edouard (1842–1891). This French mathematician worked in various areas of number theory, including Diophantine equations. He studied the Fibonacci sequence extensively, leading to a generalization called *Lucas sequences*. He also invented the Tower of Hanoi puzzle.

Mazur, Barry (1937–). This New York–born mathematician earned his Ph.D. from Princeton at the age of 21 and has been at Harvard for nearly 50 years. He is active in research and teaching and has made important

contributions on elliptic curves and other areas of number theory and mathematics.

Mordell, Louis (1888–1972). Born in Philadelphia, this British mathematician worked in number theory, advancing knowledge of rational points on elliptic curves.

Pell, John (1611–1685). This English mathematician studied Diophantine equations, though not the particular type that bears his name, which was mistakenly attributed to Pell by Gauss.

Pythagoras (c. 569–507 B.C.E.). Although best known for the theorem about right triangles that bears his name, Pythagoras had a much broader influence on mathematics and scholarship in general. Born on the Greek island of Samos, he moved to what is now southern Italy and founded a religious and scholarly community called the Brotherhood. Because they left no written records, knowledge about the "Pythagoreans" of the Brotherhood comes from later sources, including Plato and Aristotle. The Brotherhood considered numbers the basis of all reality; Pythagoras is called the "Father of Number Theory."

Ramanujan, Srinivasa (1887–1920). Born and raised in India, Ramanujan received almost no formal training in mathematics and yet is considered one of the mathematical geniuses of the 20th century. He made incredible contributions to number theory and analysis.

Riemann, Bernhard (1826–1866). A major figure in mathematics during the mid-19th century, Riemann made important contributions to analysis, geometry, and topology. Calculus students everywhere know of the Riemann integral. His Ph.D. advisor was Gauss, and he spent his brief career at the University of Göttingen. His conjecture about the distribution of primes, called the *Riemann Hypothesis*, is one of the most important unsolved questions in mathematics today.

Rivest, Ronald (1947–). This computer scientist from MIT works in cryptography. Together with Leonard Adleman and Adi Shamir, he created a method of public key encryption known as the RSA algorithm.

Selberg, Atle (1917–2007). This Norwegian mathematician won the Fields Medal in 1950 for his work relating analysis to the Riemann zeta function. He also discovered an "elementary" proof of the prime number theorem.

Shamir, Adi (1952–). This cryptographer from the Weizmann Institute in Israel created in 1977, together with Leonard Adleman and Ronald Rivest, a method of public key encryption known as the RSA algorithm.

Skewes, Stanley (1899–1988). This South African mathematician is best known for discovering Skewes number in 1933. This number gave a bound on an interval during which values related to prime numbers exhibit certain properties. At the time, this number was the largest number to have significance in a mathematical proof.

Turing, Alan (1912–1954). This British mathematician and cryptographer is considered by many to be the father of modern computer science. During World War II, his work with British intelligence was critical to cracking the Enigma encryption scheme used by the Nazis. In 1966, the Association for Computing Machinery established the Turing Award, now considered the equivalent of the Nobel Prize in the computing world.

Vallée-Poussin, Charles Jean de la (1866–1962). This Belgian mathematician independently produced a proof of the prime number theorem in 1896, the same year that Jacques Hadamard also produced a proof.

Wiles, Andrew (1953–). This British mathematician on the Princeton faculty worked for nearly 10 years to prove a result involving elliptic curves that finally proved Fermat's Last Theorem in 1993. He has received many awards, including the Cole Prize and Wolf Prize.

Bibliography

Burger, Edward B. *Student Mathematical Library. Vol. 8, Exploring the Number Jungle: A Journey into Diophantine Analysis*. Providence: American Mathematical Society, 2000. Focuses on discovering the hidden truths and treasures of Diophantine analysis.

———. *Zero to Infinity: A History of Numbers*. Chantilly, VA: The Teaching Company, 2007. A 24-lecture video of the history of numbers that sets up the background for this course.

Burger, Edward B. and Robert Tubbs. *Making Transcendence Transparent: An Intuitive Approach to Classical Transcendental Number Theory*. Cambridge: Springer, 2004. An introduction to the challenging field of transcendental number theory.

Hardy, G. H. and E. M. Wright. *An Introduction to the Theory of Numbers*. 5th ed. New York: Oxford University Press, 1980. A good overall introduction.

Niven, Ivan, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers*. New York: John Wiley & Sons, Inc., 1991. Another good overall introduction.

Stark, Harold M. *An Introduction to Number Theory*. Cambridge: MIT Press, 1978. A useful overview.

Answers to Selected Questions to Consider

Lecture One

1. Courtroom proceedings, crafting legislation, contract negotiations.
2. Argue by contradiction: Suppose the number 21 is *not* interesting. Then, because we are supposing that the numbers 1 through 20 *are* interesting, we find that 21 is the smallest *un*interesting number. But this makes 21 interesting! We have a contradiction to our assumption about 21, and thus 21 must be interesting.

Lecture Two

1. The number 64 is a perfect square: $64 = 8 \times 8$. It is also a perfect cube: $64 = 4 \times 4 \times 4$. In fact, 64 is a power of 2: $64 = 2 \times 2 \times 2 \times 2 \times 2 \times 2 = 2^6$. The number 61 is neither a perfect square nor cube. It does not have 2 as a factor and so is odd. Not only that, 61 has no factors other than itself and 1.
2. Following the algorithm in the lecture, we generate the following sequence: 7, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1, and now it becomes periodic.

Lecture Three

1. Using our formula, we have: $(1{,}000{,}000 \times 1{,}000{,}001)/2 = 500{,}000{,}500{,}000$.
2. Look the table below for values for several pairs of consecutive triangular numbers. Notice the amazing pattern!

Triangular numbers	Squares	Differences of squares	Perfect cubes!
1	1		
3	9	$9 - 1 = 8$	$8 = 2^3$
6	36	$36 - 9 = 27$	$27 = 3^3$
10	100	$100 - 36 = 64$	$64 = 4^3$
15	225	$225 - 100 = 125$	$125 = 5^3$
21	441	$441 - 225 = 216$	$216 = 6^3$

Lecture Four

1. The suggested hint points out that this progression can be obtained from the progression 1, 5, 25, 125, ... after we multiply each term by −2. So we will first find the sum of the first five terms of the progression 1, 5, 25, 125, ... Using the notation from the lecture, we notice that this progression has $r = 5$, so the sum of the first five terms is $(5^5 - 1)/(5 - 1) = 3124/4 = 781$. We now multiply this answer by −2 to find that the sum of the first five terms of our original progression is −1562.
2. We notice that the given infinite geometric series can be obtained from the infinite geometric series $1 + 1/10 + 1/100 + 1/1000 + \cdots$ after we multiply the entire sum by 9/10. So we will first find the sum of the infinite series $1 + 1/10 + 1/100 + \cdots$, which has an r value equal to 1/10. The formula in the lecture gives us a sum of $1/(1 - r) = 1/(1 - 1/10) = 10/9$. We now multiply this answer by 9/10 to find that the sum of our original progression is 1. Thus we have shown that 0.999... = 1. Amazing (and correct)!

Lecture Five

1. a) The pattern explored in the lecture suggests that the sum of the first n Fibonacci numbers is 1 less than the Fibonacci number two steps further down the list. So the sum of the first 10 Fibonacci numbers should be 1 less than the 12th Fibonacci number, which is 144. Thus our desired sum equals 143.

   b) The largest Fibonacci number less than 100 is 89, so we have $100 = 89 + 11$. We see easily that $11 = 8 + 3$, two more Fibonacci numbers, giving us $100 = 89 + 8 + 3$. We replace each term in this sum with its Fibonacci successor (a number approximately 1.6 times as large) to get $144 + 13 + 5 = 162$. So 100 miles is approximately 162 kilometers.
2. N/A

Lecture Six

1. This sequence begins with seed values 1 and 1. Successive terms are obtained as follows: Multiply the most recent term by 3 and add the result to the term that came before. Thus $4 = 3 \times 1 + 1$, $13 = 3 \times 4 + 1$, $43 = 3 \times 13 + 4$, and so on.

2. We use the general formula given in the lecture: The puzzle with n disks requires $2^n - 1$ moves. With $n = 10$, we need $2^{10} - 1 = 1023$ moves.

Lecture Seven

1. We consider the product $2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 17 \times 19$ and then add 1. Because this number has remainder 1 when divided by each prime, 2, 3, 5, 7, 11, 13, 17, and 19, and because 20 itself is not a prime, any prime factors of this large product (plus 1) must be greater than 20. But we know this number is either itself prime or can be written as a product of primes, hence in either case there must exist a prime greater than 20.
2. The number $101 \times 100 \times 99 \times 98 \times 97 \times \cdots \times 3 \times 2 \times 1$ can be written compactly as "101!" (read "101 factorial"). Clearly the numbers 2, 3, 4, ... , 101 are factors of 101!. Thus we observe that $101! + 2$ has 2 as a factor, $101! + 3$ has 3 as a factor, $101! + 4$ has 4 as a factor, and so on, up to $101! + 101$, which has 101 as a factor. Therefore we have 100 consecutive natural numbers: $101! + 2$, $101! + 3$, $101! + 4$, $\cdots$, $101! + 101$, each of which is composite. (Note: We do not claim that this list is the *smallest* 100 consecutive composite numbers, but it is a list of 100 consecutive numbers that we are *certain* are all composite!)

Lecture Eight

1. Because every 7th natural number is a multiple of 7, the probability that a natural number chosen at random is a multiple of 7 is 1/7. Thus, the probability that a natural number is *not* a multiple of 7 is $1 - 1/7 = 6/7$.
2. We must sum the first 4 terms in the series to get a partial sum greater than 2, and we must sum 11 terms to exceed 3.

Lecture Nine

1. No such progression of primes exists. Here is why: If we start with $n = 2$, then $n + 3 = 5$, which is prime, but $n + 6 = 8$, which is not. All other primes are odd. But if n is odd, then $n + 3$ would be an even number greater than 2 and thus cannot be prime.
2. We produce Fermat primes for $n = 1$ and $n = 2$ as follows: $2^{2^1} + 1 = 2^2 + 1 = 5$ and $2^{2^2} + 1 = 2^4 + 1 = 17$. (Note that when $n = 3$, the formula yields 129, which has a factor of 3 and therefore is not prime.)

Lecture Ten

1. Because the number 123,456,789 − 213 has a factor of 123, we know that the numbers 123,456,789 and 213 must have the *same* remainder when divided by 123. So to answer the question, we take the easy way out and simply divide 123 into 213. We get a quotient of 1 and a remainder of 90, which must also be the remainder after dividing 123,456,789 by 123.
2. N/A

Lecture Eleven

1. N/A
2. Because 29 has no common factors with 31, Fermat's Little Theorem tells us that $29^{30} \equiv 1 \pmod{31}$, so the remainder is 1 (notice that the exponent 30 equals 31 − 1).

Lecture Twelve

1. We note that of all the possible remainders when dividing by 12: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, and 11, only 4 of them are relatively prime to 12: 1, 5, 7, and 11. So by the extension of Fermat's Little Theorem due to Euler, because 7 is relatively prime to 12, we have $7^4 \equiv 1 \pmod{12}$.
2. N/A

Lecture Thirteen

1. Suppose the integers x, y, and z formed a solution to the equation. The left side would be an integer that when divided by 3 gives a remainder of 0. But the right side would be an integer that gives a remainder of 2 when divided by 3. This is impossible, so no such integer solution exists.
2. Fermat's method of ascent as applied to this equation gives formulas for obtaining a new solution from an old one: $x_{new} = 3x_{old} + 4y_{old}$ and $y_{new} = 2x_{old} + 3y_{old}$. These formulas were used in the lecture to generate the solution $x = 17$ and $y = 12$ from the solution $x = 3$ and $y = 2$. We now substitute $x_{old} = 17$ and $y_{old} = 12$ into the formulas to obtain a third solution: $x_{new} = (3 \times 17) + (4 \times 12) = 99$ and $y_{new} = (2 \times 17) + (3 \times 12) = 70$. It is easy to check that $99^2 - (2 \times 70^2) = 1$, so this new solution does work.

Lecture Fourteen

1. Suppose, contrary to what we wish to establish, that we had a triple of natural numbers x, y, and z that satisfied $x^{100} + y^{100} = z^{100}$. This equality is equivalent to the equation $(x^{20})^5 + (y^{20})^5 = (z^{20})^5$, giving us natural numbers x^{20}, y^{20}, and z^{20} satisfying the equation $x^5 + y^5 = z^5$. This is a contradiction since we know that it has been shown that there are no natural numbers that satisfy this Diophantine equation, so our assumption is false, and therefore no natural-number solution to $x^{100} + y^{100} = z^{100}$ exists.
2. The next Germain prime is 23. We note that $2 \times 23 + 1 = 47$, which is indeed prime. It is easy to check that none of the primes between 11 and 23 are Germain primes. For example, 13 is not a Germain prime because $2 \times 13 + 1 = 27$, which is not prime.

Lecture Fifteen

1. There are two ways to factor 100 into "primes" in the ring of even integers: $100 = 10 \times 10$, and $100 = 2 \times 50$.
2. N/A.

Lecture Sixteen

1. The length you measure should equal 5 inches. You are measuring the sides of what should be a right triangle, so the length of the hypotenuse squared should be the sum of the squares of the other two lengths, in this case, $3^2 + 4^2 = 25$.
2. Because this method generates a different Pythagorean triple for each natural number greater than 1 and there are infinitely many such numbers, you have shown that there are infinitely many such triples.

Lecture Seventeen

1. The point $(-1, 0)$ is on the line because substituting $x = -1$ and $y = 0$ into equation $y = 1/2(x + 1)$ gives a valid equation. To find the second point where this line intersects the unit circle, we use the formulas derived in the lecture: $X = (1 - m^2)/(1 + m^2)$, and $Y = 2m/(1 + m^2)$. The value of m is the slope of our line; in this case $m = 1/2$. Substituting into our formulas, we obtain $X = (1 - (1/2)^2)/(1 + (1/2)^2) = (1 - 1/4)/(1 + 1/4) = 3/5$ and $Y = 2(1/2)/(1 + (1/2)^2) = 1/(1 + 1/4) = 4/5$. So the second point is $(3/5, 4/5)$.

2. Substituting $x = 8/17$ and $y = 15/17$ into $x^2 + y^2 = 1$, we get $(8/17)^2 + (15/17)^2 = 64/289 + 225/289 = 289/289 = 1$. Thus the given point does lie on the unit circle. The corresponding Pythagorean triple is (8, 15, 17).

Lecture Eighteen

1. For the point (1, 1), we substitute $x = 1$ and $y = 1$ into the equation to obtain $1 = 1 - 1 + 1$, which is valid. For the point (0, 1), we substitute $x = 0$ and $y = 1$ to obtain $1 = 1$, which is also valid.
2. Setting $y = 0$, the equation becomes $0 = x^3 - 4x$. The right side factors to yield $0 = x(x^2 - 4) = x(x - 2)(x + 2)$. The three factors on the right multiply to give 0, so one of them must be 0. Thus we have $x = 0$, $x = 2$, or $x = -2$.

Lecture Nineteen

1. We suppose $\sqrt{3}$ is rational and work toward a contradiction. If $\sqrt{3}$ is rational, then $\sqrt{3} = a/b$ for some integers a and b. So $3 = a^2/b^2$, and thus $3b^2 = a^2$. Recall that every natural number can be written uniquely as a product of primes. Note also that 3 is prime and that 3 must appear an even number of times in the prime factorizations of a^2 and b^2. But then the equation $3b^2 = a^2$ would have an odd number of 3s dividing the left side and an even number of 3s dividing the right side, which is impossible. Thus our original assumption must have been faulty, and so $\sqrt{3}$ is irrational.
2. Given that α is an irrational number, we know that its decimal expansion never terminates or becomes periodic. The decimal expansion for 10α is obtained from the expansion for α by moving the decimal point one digit to the right. Thus 10α also has a non-terminating, non-periodic expansion, and therefore it must also be irrational.

Lecture Twenty

1. We have $4x = 0 - 5$, so $4x = -5$, and thus $x = -5/4$.
2. We know that raising $1/\sqrt[3]{2}$ to the third power yields 1/2. Therefore $x = 1/\sqrt[3]{2}$ satisfies the equation $x^3 - 1/2 = 0$. To obtain integer coefficients, we multiply through by 2 to obtain $2x^3 - 1 = 0$.

Lecture Twenty-One

1. The first such power is 46: $2^{46} = 70{,}368{,}744{,}177{,}664$. (Please note that this may be difficult to verify without a calculator or software that carries at least 14 significant digits.)
2. Comparing the decimal expansions of 22/7 and 31/10 to that of π:

$$\pi = 3.14159265\ldots$$
$$22/7 = 3.14285714\ldots$$
$$31/10 = 3.10000000\ldots$$

we see that 22/7 is accurate to two decimal places, whereas 31/10 is accurate to only one. Dirichlet's Theorem from the lecture also tells us that 22/7 lies within 1/56 of π. In addition, 22/7 uses a smaller denominator than 31/10, and so is "less expensive."

Lecture Twenty-Two

1. We compute:

$$\frac{18}{7} = 2+\frac{4}{7} = 2+\frac{1}{7/4} = 2+\frac{1}{1+3/4} = 2+\frac{1}{1+\frac{1}{4/3}} = 2+\frac{1}{1+\frac{1}{1+\frac{1}{3}}}.$$

2. Using a calculator, we find $e = 2.7182818284\ldots$. Thus:

$$e = 2+\frac{1}{1/0.781828182845905\ldots} = 2+\frac{1}{1.39221119117733\ldots}$$
$$= 2+\frac{1}{1+\frac{1}{1/0.39221119117733\ldots}} = 2+\frac{1}{1+\frac{1}{2.54964677830384\ldots}}$$
$$= 2+\frac{1}{1+\frac{1}{2+\frac{1}{1/0.54964677830384\ldots}}} = 2+\frac{1}{1+\frac{1}{2+\frac{1}{1.81935024359809\ldots}}}$$

and continuing in this manner reveals the first few partial quotients.

Lecture Twenty-Three

1. We note that: $\sqrt{5} = 2+\cfrac{1}{4+\cfrac{1}{4+\cfrac{1}{4+\cfrac{1}{4+\ddots}}}}$.

The next three best rational approximants are:

$$2+\frac{1}{4} = \frac{9}{4},\quad 2+\frac{1}{4+\frac{1}{4}} = 2+\frac{1}{17/4} = 2+\frac{4}{17} = \frac{38}{17},\text{ and}$$

$$2+\frac{1}{4+\frac{1}{4+\frac{1}{4}}} = 2+\frac{1}{4+\frac{1}{17/4}} = 2+\frac{1}{4+\frac{4}{17}} = 2+\frac{1}{72/17} = 2+\frac{17}{72} = \frac{161}{72}$$

2. As described in the lecture, we look at each rational approximant as a fraction x/y. So first we have $x = 9$ and $y = 4$. Substituting into the given Pell equation, we see $(9)^2 - 5(4^2) = 81 - 80 = 1$, so $x = 9$ and $y = 4$ is a solution. Because we learned that every other approximant is a solution n, we now check $x = 161$ and $y = 72$ to find $(161)^2 - 5(72^2) = 25{,}921 - 25{,}920 = 1$. Thus $x = 161$ and $y = 2$ is also a solution.

Lecture Twenty-Four

1. N/A.
2. N/A.